Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: 1 February 2019
Project duration: 47 months

Cyber Security for Europe

D6.6

Final Educational and Assessment Framework

Document Identification	
Due date	31 July 2022
Submission date	8 July 2022
Revision	1.0

Related WP	WP6	Dissemination Level	PU
Lead Participant	DTU	Lead Author	Alberto Lluch Lafuente (DTU)
Contributing Beneficiaries	KAU, UNITN, JAMK, UMU, VTT, POLITO	Related Deliverables	D6.1, D6.2, D6.3, D6.4, D6.5

Abstract The European Union needs to ensure that highly skilled engineers, scientists and other specialists in all areas of cybersecurity are educated throughout their lifetime to implement, support and lead solutions regarding current and future industrial, scientific, societal and political challenges related to cybersecurity. To support the EU in this challenge, CyberSec4Europe has developed an education and assessment framework of CyberSec4Europe, presented in this deliverable. The aim of the framework is not to *produce all possible content* required to implement educational and training programmes, but instead to *define guidelines and tools that support the design of capability building instruments*, open to external sources and third-party material outside the consortium, that in particular contain guidelines and methodologies to ensure adequate quality standards. This includes the identification of cybersecurity knowledge units and curricula, the specification of learning objectives and competences required to develop and enhance cybersecurity skills for different profiles and roles, the development of training and awareness to achieve such objectives and competences, together with activities to apply and test such competencies.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

This deliverable presents the education and assessment framework of CyberSec4Europe, which aims to serve as a support for continuing education and lifelong training. The aim of the framework is not to *produce all possible content* required to implement educational and training programmes, but instead to *define guidelines and tools that support the design of capability building instruments*, open to external sources and third-party material outside the consortium, that in particular contain guidelines and methodologies to ensure adequate quality standards. This includes the identification of cybersecurity knowledge units and curricula, the specification of learning objectives and competences required to develop and enhance cybersecurity skills for different profiles and roles, the development of training and awareness to achieve such objectives and competences, together with activities to apply and test such competencies.

Section 2 addresses the question "What are the knowledge areas, units and skills that can be taught (in general)?" by presenting the CyberSec4Europe Knowledge Framework [D6.2], which provides a unifying structure and terminology for cybersecurity knowledge areas, topics and skills, intended to serve as solid common ground for designing and assessing education and training in cybersecurity, whichever its sector of application.

Section 3 addresses the questions "What are the knowledge areas, units and skills that should be taught for specific purposes?" and "how should an education unit be designed and offered?". The first question is addressed by summarising and extending on a cybersecurity skill evaluation methodology for job profiles initially presented in [D6.3]. To address the second question we provide suggestions to incorporate research and demonstrators results of CyberSec4Europe into future educational offers. Moreover, we explain how non-traditional education formats such as cyberranges, serious games and Massive Online Open Courses (MOOCs) can be used to offer suitable cybersecurity learning experiences.

Finally, Section 4 addresses the question "How does one assess and evaluate the quality of an education offer?". We first summarise our quality-criteria based approach to evaluating single education units offered as MOOCs. We then report on an online survey that we conducted to analyse the role of cybersecurity MOOC certification based on the proposed quality criteria for cybersecurity. Last, we present a quality branding process for cybersecurity MOOCs.

Overall, this deliverable provides an overview over most of the education and training activities that have been carried out within CyberSec4Europe. This includes curated summaries of key contributions presented in previous deliverables [D6.1,D6.2,D6.3,D6.4,D6.5], as well as novel contributions, including translations from our framework to the European Cybersecurity Education and Professional Training Minimum Reference Curriculum (ECSO) occupations and skills standard, guidelines to develop Security Serious Games (SSG) and other gamification approaches to education, studies on job profiles of long prevalence in the cybersecurity field (border control), and incidence of current research initiatives into the knowledge areas defined in our framework.

Document information

Contributors

Name	Partner
Alberto Lluch Lafuente	DTU
Koen Tange	DTU
Simone Fischer-Hübner	KAU
Matthias Beckerle	KAU
Carlos Esteban Budde	UNITN
Silvia Vidor	UNITN
Fabio Massacci	UNITN
Jani Päijänen	JAMK
Anni Karinsalo	VTT
Antonio Skarmeta	UMU
Andrea Atzeni	POLITO

Reviewers

Name	Partner
Stephan Krenn	AIT
Christine Jamieson	TDL
Marco Crabu	ABI LAB

History

Version	Date	Authors	Comment
0.01	2021-10-18	Alberto Lluch Lafuente, Carlos E. Budde	1st Draft by DTU and UNITN with agreed ToC
0.02	2021-10-27	Alberto Lluch Lafuente	ToC refined to subsection level
0.03	2021-12-14	Alberto Lluch Lafuente	Plan with dates, page limits and responsibilities.
0.04	2022-02–02	Various	First draft of some sections
0.05	2022-06-13	Various	First complete draft
1.00	2022-07-07	Koen Tange, Carlos E. Budde	Final version, incorporating internal review feedback

Table of Contents

List of Figures

List of Tables

List of Acronyms

A	**ACM**	Association for Computer Machinery (US)
C	**CSEC**	Cybersecurity Curricular Guidelines
	CWF	Cybersecurity Workforce Framework
	CyBOK	Cybersecurity Body of Knowledge (UK)
D	**DDoS**	Distributed Denial of Service
E	**ECSO**	European Cybersecurity Education and Professional Training Minimum Reference Curriculum
	ESCO	European Skills/Competences, qualifications and Occupations
	EES	Entry Exit System
I	**IEEE**	Institute of Electrical and Electronics Engineers (US)
J	**JRC**	Joint Research Centre
M	**MOOC**	Massive Open Online Course
N	**NIST**	National Institute of Standards and Technology (US)
S	**SSG**	Security Serious Games

1 Introduction

The European Union needs to ensure that highly skilled engineers, scientists and other specialists in all areas of cybersecurity are educated throughout their lifetime, to implement, support and lead solutions regarding current and future industrial, scientific, societal and political challenges related to cybersecurity.

This goal leads to the following main questions:

- What are the knowledge areas, units and skills that can be taught (in general)?
- What are the knowledge areas, units and skills that should be taught for specific purposes?
- How should an education unit be designed and offered?
- How does one assess and evaluate the quality of an educational offer?

One of the goals of CyberSec4Europe is to define and propose an education and assessment framework that addresses those questions, and that serves as a support for continuing education and lifelong learning in all the mentioned areas of cybersecurity.

The aim of the framework is not to *produce all possible content* required to implement educational and training programmes, but instead to *propose and define guidelines and tools that support the design of capability building instruments*, open to external sources and third-party material outside the consortium, that in particular contain criteria and methodologies to ensure adequate quality standards. This includes the identification of cybersecurity knowledge units and curricula, the specification of learning objectives and competences required to develop and enhance cybersecurity skills for different profiles and roles, the development of training and awareness to achieve such objectives and competences, together with activities to apply and test such competencies.

1.1 Content and outline of this document

Cybersecurity is a vast and rich interdisciplinary field that encompasses many different sectors, concepts, techniques, methodologies and tools. This makes it challenging to clearly pinpoint and agree on knowledge concepts—i.e. terminology and categorisation of "educational units"—to be used as the foundation of cybersecurity education curricula. To this aim, Section 2 addresses the question "What are the knowledge areas, units and skills that can be taught (in general)?" by presenting the CyberSec4Europe Knowledge Framework [D6.2]. This provides a unifying structure and terminology for cybersecurity knowledge areas, topics and skills, intended to serve as solid common ground for designing and assessing education and training in cybersecurity, whichever its sector of application.

Such a framework permits a subsequent unambiguous discussion of the following key question: "What are the knowledge areas, units and skills that should be taught for specific purposes?" To answer this question, Section 3 summarises and extends on a cybersecurity skill evaluation methodology for job profiles initially presented in [D6.3]. This exercises the framework—showing its use by cybersecurity and domaiwn experts to identify the relevant knowledge units of strategically-chosen job profiles—by determining how important those units are for the required skills of the profiles.

However, since cybersecurity is a fast moving field, education programmes must be continuously updated with state-of-the-art research and innovation knowledge to keep training up-to-date and relevant. Therefore, and to answer the third question: "How should an education unit be designed and

offered?", Section 3.2 provides suggestions to incorporate research and demonstrator results of CyberSec4Europe into future educational offers. Moreover, in Section 3.3 we explain how non-traditional education formats such as cyber ranges, serious games and MOOCs can be used to offer suitable cybersecurity learning experiences.

Finally, Section 4 addresses the question "How does one assess and evaluate the quality of an educational offer?". We first summarise our quality-criteria based approach to evaluating single education units offered as MOOCs. We then report on an online survey that we conducted to analyse the role of cybersecurity MOOC certification based on the proposed quality criteria for cybersecurity. Last, we present a quality branding process for cybersecurity MOOCs.

Overall, this deliverable provides an overview of the most relevant activities related to education and training carried out within CyberSec4Europe. This includes curated summaries of key contributions presented in previous deliverables [D6.1, D6.2, D6.3, D6.4, D6.5], as well as novel contributions—expanded in the appendices and references—of which the most prominent are:

1. Translations from our framework to the ESCO occupations and skills standard.
2. Guidelines to develop SSG and other gamification approaches to education.
3. Studies on job profiles of long prevalence in the cybersecurity field (e.g. border control).
4. Incidence of current research initiatives into the knowledge areas defined in our framework.

2 The CyberSec4Europe Cybersecurity Knowledge Framework

Cybersecurity is a vast and rich interdisciplinary field that encompasses many different concepts, techniques, methodologies and tools. The CyberSec4Europe Knowledge Framework aims to provide a unifying structure and terminology for cybersecurity knowledge areas, topics and skills, intended to serve as solid common ground for designing and assessing education and training in cybersecurity.

2.1 Cybersecurity Knowledge Frameworks

Several cybersecurity frameworks have been developed over the last five years (i.e. from 2017 to 2022), aimed at providing suitable reference structures for different purposes: academic education, professional training, and scientific and technological research. We mention in particular the following frameworks, due to the broadness of their scope and the well-established international institutions that produced them:

- The Cybersecurity Curricular Guidelines (CSEC) [ACM17].
- The Cybersecurity Workforce Framework (CWF) [NIST17].
- The European Cybersecurity Taxonomy (JRC) [JRC19].
- The Cybersecurity Body of Knowledge (CyBOK) [CyBOK19].
- The European Cybersecurity Education and Professional Training Minimum Reference Curriculum (ECSO) [ECSO21].

Table 1 gives an overview of these frameworks, where we highlight their main focus and how cybersecurity knowledge is structured.

Table 1: Cybersecurity knowledge frameworks

Framework	Proposers	Focus	Structure
CSEC	ACM, IEEE-CS, AIS SIGSEC, IFIP WG 11.8	Academic curriculum	8 Knowledge Areas / 54 Knowledge Units
CWF	NIST	Workforce skills	7 categories / 33 specialty areas
JRC	JRC	Research and technology	15 research domains / 150 subdomains
CyBOK	NCSC	Scientific knowledge	19 Knowl. Areas / 244 topics
ECSO	ECSO	Workforce skills	4 modules / 17 subjects

Each of these frameworks provides, from its own perspective, a comprehensive structured view on the cybersecurity landscape. As these views are complementary, considering all frameworks draws an overarching picture of the cybersecurity panorama. More specifically, the CSEC framework is aimed at structuring academic curricula, while the ECSO and CWF frameworks focus on professional training and workforce skills. In turn, the CyBOK framework structures mainly scientific knowledge—rather than pedagogical approaches—while the JRC framework is focused on research and technology. Although complementary, these multiple perspectives also result in a significant overlap of concepts and terminology. Detailed descriptions and comparisons of the frameworks are in [D6.2] and [D6.3].

2.2 The CyberSec4Europe Knowledge Framework

The CyberSec4Europe Knowledge Framework combines ideas from the above listed frameworks. In particular, the CSEC framework has been used as the main foundation, and it has been enriched with profession-oriented components from the CWF framework. For our purposes, CSEC provides arguably the best basis since it uses the recognized and well-established scientific terminology from the ACM, making it suitable for education and training personnel.

The resulting framework is summarised in Table 2, where each knowledge area is broken down into several smaller knowledge units. All knowledge areas are taken from CSEC but one: the knowledge area "operate and maintain" and its corresponding knowledge unit "Customer Service and Technical Support", stem from CWF. A detailed analysis of the relation of terminology and concepts of CSEC and CWF can be found in [D6.2].

Table 2: The CyberSec4Europe knowledge framework

Knowledge Area	Knowledge Unit
Data security	Cryptography, digital forensics, data integrity and authentication, access control, secure communication protocols, cryptanalysis, data privacy, information storage security.
Software security	Fundamental principles, design, implementation, analysis and testing, deployment and maintenance, documentation, ethics.
Component security	Component design, component procurement, component testing, component reverse engineering.
Connection security	Physical media, physical interfaces and connectors, hardware architecture, distributed systems architecture, network architecture, network implementations, network services, network defence.
System security	System thinking, system management, system access, system control, system retirement, system testing, common system architectures.
Human security	Identity management, social engineering, personal compliance with cybersecurity rules/policy/ethical norms, awareness and understanding, social and behavioural privacy, personal data privacy and security, usable security and privacy
Organisational security	Risk management, security governance and policy, analytical tools, systems administration, cybersecurity planning, business continuity (including disaster recovery and incident management), security program management, personnel security, security operations.
Operate and maintain	Customer service and technical support.
Societal security	Cybercrime, cyber law, cyber policy, privacy.

3 Cybersecurity Education Design Framework

In this Section, we aim to answer two questions. Firstly, what are the knowledge areas, units and skills that should be taught for a specific purpose? And secondly, how should an education unit be designed and offered?

To answer the first question, we summarise and extend on a cybersecurity skill evaluation methodology for job profiles initially presented in [D6.3]. The key idea of this methodology is to identify the relevant knowledge units (of the framework presented in Section 2) by determining how important those units are for the definition of the required skills of the profiles.

However, since cybersecurity is a fast moving field, education programmes must be continuously updated with state-of-the-art research and innovation knowledge to keep training up-to-date and relevant. Therefore, and to answer the second question, we provide in Section 3.2 suggestions to incorporate CyberSec4Europe's results into future education offers. Finally, Section 3.3 explains how non-traditional education formats such as cyber ranges, serious games and MOOCs can be designed to offer suitable cybersecurity learning experiences, focusing mainly on the relevant developments carried out within CyberSec4Europe.

3.1 Designing Education: from skills to content

In [D6.3], we presented a methodology for evaluating cybersecurity skills for professionals based on the CyberSec4Europe Assessment Framework. We demonstrated the applicability of our methodology in several use cases, assessing in total 18 job profiles, organised in interactive scenarios for each use case. Besides IT professionals, our demonstration also included non-ICT workforce. In particular, we provided examples in applying the framework to lawyers. An illustration of the framework and how it was used is presented in Figure 1. The table shows a set of profiles in relation to the knowledge units. For each profile and each knowledge unit, the numbers indicate the relevance of the unit for the specific on a scale from 0 (not relevant) to 3 (very relevant), as assessed by a group of experts. A summary and analysis of the results can be found in [D6.3].

	Knowledge area	Data Security					
Profile / Description	**Knowledge unit**	**Cryptography**	**Digital Forensics**	**Data Integrity and Authentication**	**Access Control**	**Secure Communication Protocols**	**Cryptanalysis**
General Cybersec Auditor	Person in charge of conducting an external or internal audit of security controls and information systems. Person is also responsible of updating security policies.	1	2	2	2	2	1
Technical Cybersec Auditor	This Job profile would be an escalation level for the general cybersec auditor. The work includes providing in-depth analysis of where the cybersecurity systems are adequate and operating well, as well as where there is room for or a need for improvement. If enhancements are required, the security auditor may also be responsible for providing an analysis of recommended security measures.	2	3	3	3	3	2
Threat Modelling Engineer	The job profile focuses on establishing security requirements, locating security risks and potential vulnerabilities, calculating threat and vulnerability criticality, and prioritizing remedial options. Making well-documented threat models gives assurances that may be used to explain and defend an application system's security	2	2	3	2	3	2

Figure 1: An illustration of the use of the framework

Our evaluation of the methodology continued beyond [D6.3] to demonstrate the applicability of the framework beyond the current-day needs of European actors, in order to address future directions of

cybersecurity. For this we devised and analysed a border-control scenario and related long-term (cybersecurity-relevant) job profiles, and evaluated them with the assessment framework of CyberSec4Europe. We drew inspiration from the European-level cybersecurity skill advancement ECSO, which has built a framework for the purpose of cybersecurity skills and competence development of professionals [ECSO21]. The full list of the 6 profiles used in this extended evaluation of the framework can be found in Annex A: Job Profile Assessment. The details of our evaluation are included below in section 3.1.1.

In addition, we have mapped the knowledge units defined in the CyberSec4Europe Assessment Framework to the later-published European Skills/Competences, qualifications and Occupations (ESCO). ESCO is a standard for the classification of European work positions and the skills required to perform in them. Thus, our mapping from the CyberSec4Europe framework to ESCO approaches the educational design from the opposite end with respect to our job profiles assessments. In particular, it facilitates the interpretation of our assessments—i.e. which skills are relevant for which jobs—in "common ground" that can be picked up, for example, by universities defining their cybersecurity curricula. Technically, to create this mapping, we have filtered a list of essential and optional skills from ESCO, that are necessary in the cybersecurity profession. Table 14 in Annex B: ESCO Skills presents the list of essential and optional skills divided for each profile defined in the framework, while Table 15 lists the skills identified through this selection.

3.1.1 Evaluation of long-term job profiles

We present here the extended evaluation of our methodology on the above mentioned 6 long-term cybersecurity job profiles. Firstly, we present a use case related to EU border control context, the workflow of which is depicted in Figure 2. A scenario of the use case is implemented. We define four job profiles relevant in that specific scenario. Lastly, we evaluate the related skill requirements within each job profile. The evaluation summaries are presented in Annex A: Job Profile Assessment. In addition, to extend the long-term profile evaluations within the scope of our use case, we evaluate two additional job profiles extrapolated from items defined in the ECSO Minimal Reference Curricula published ECSO [ECSO21].

Use case: Border control intra-EU

Since border control posts typically utilise threat models to reduce risk, these models affect how and what kind of threats the security personnel are looking for in the system. In addition to detection mechanisms such as biometric identification and automated passport control readers, the access of unauthorised passengers is dependent on the threat model that is designed, i.e. how the border control personnel are prepared to identify the unauthorised passengers. False positives in the system might be hard to notice without a proper indicator. Therefore, the chosen threat model—that is employed to detect unauthorised passengers—affects the probability of them being allowed access mistakenly.

Figure 2. Workflow of the EES

The scenario is about applying and auditing the threat model to border crossing check-points at the airport. This consists of the application of potentially new threat models, which will be realised by border guards in the border control point. The actual threat model will be validated and enforced by four

profiles, described in the following consecutive sections. These job profiles represent central cybersecurity actors in the specific scenario:

- General cybersecurity auditor (in the case of Entry Exit System (EES))
- Technical cybersecurity auditor
- Threat modelling engineer
- Security engineer

Job profile: General cybersecurity auditor: This job profile in the case of border control can be looked at within the context of auditing the Entry/Exit System (EES) that is in the process of being implemented in all EU countries to ease manual border control checks. The EES is an automated IT system for registering third-country visitors, both those with short-stay visas and those who do not require a visa, whenever they cross an EU external border. The person's name, type of travel document, biometric data, and the date and location of entry and exit are recorded by the system. The knowledge, skill set and responsibilities for this profile are listed in Table 3.

Job profile: Technical cybersecurity auditor: This job profile can be described as a (technical) specialisation of the general cybersecurity auditor. The work includes providing in-depth analysis of where the cybersecurity systems are adequate and operating well, as well as where there is room for improvement. If enhancements are required, the security auditor may also be responsible for providing an analysis of recommended security measures. The knowledge, skill set and responsibilities for this profile are listed in Table 4.

Job profile: Threat modelling engineer: This job profile focuses on establishing security requirements, locating security risks and potential vulnerabilities, calculating threat and vulnerability criticality, and prioritising remedial options. Creating well-documented threat models gives assurances that may be used to explain and defend an application system's security posture. The knowledge, skill set, and responsibilities for this profile are listed in Table 5.

Job profile: Security engineer: A security engineer's main job is to create and enforce security strategies and standards. The majority of the task entails predicting network or computer vulnerabilities and determining how to address them. A difference with respect to the "Technical cybersecurity auditor" is that an engineer can be in charge of implementing the cybersecurity system, while the auditor can either suggest a fitting policy, or assess the one in practice. The knowledge, skill set, and responsibilities for this profile are listed in Table 6.

Table 3: General cybersecurity auditor job profile.

Requirement	Description
Required Knowledge	Information systems and security, Risk management and assessment, Vulnerability identification
Needed skill set	Internal auditing, Audit planning, Information systems, Risk assessment, Information security, Up-to-date knowledge of threats and tactics, Problem solving
Job responsibilities	Conducting an external or internal audit of security controls and information systems, Evaluating the safety and efficacy of particular cybersecurity components of the EES, Executing cybersecurity audits, Composing technical reports that evaluate and interpret audit findings, Keeping up to date cybersecurity policies and standards, Policy development

Table 4: Technical cybersecurity auditor job profile.

Requirement	Description
Required Knowledge	Information systems and security, Risk management and assessment, Vulnerability identification, Networking, Penetration testing and security assessment of information systems
Needed skill set	Up-to-date knowledge of threats and tactics, Information security, Ability to identify risky IT procedures, Experience with risk management and mitigation, Technical skills required to assess the status of networks and systems, Ability to develop recommendations for heightened security
Job responsibilities	Ability to identify risky IT procedures, Penetration testing of the systems, Machine auditing regarding IO security, Audit of internal and external components of the kiosk machine

Table 5: Threat modelling engineer job profile.

Requirement	Description
Required Knowledge	General knowledge of computer forensics, Government and jurisprudence as they relate to cybersecurity, Operating systems, Computer network defence systems, Risk analytics and modelling, Information systems and network security and infrastructure design
Needed skill set	Incident management, Up-to-date knowledge of threats and tactics, Vulnerability assessment, Ability to identify network attacks and systemic security issues
Job responsibilities	Analysing security risks within the identification process in border control, Analysing potential risks and vulnerabilities with the EES and other systems used by the border guards

Table 6: Security engineer job profile.

Requirement	Description
Required Knowledge	Data Structures, Forensic Examination and Analysis, Knowledge of current information security trends Knowledge of cyber laws and compliance, Good networking knowledge, Incident Handling and Breaches, Analytical skills, Ability to test for, track, and resolve threats including malfunctions and attacks, Documentation writing and follow up
Needed skill set	Incident Handling and Breaches, Analytical skills, Ability to test for, track, and resolve threats including malfunctions and attacks, Documentation - writing and following up on it

Job responsibilities	To evaluate issues alerted from the security guards regarding issues with authentication of suspicious ID cards as well as other electronic travel documents, To address different network and computer vulnerabilities which could be used for malicious purposes , like performing a Distributed Denial of Service (DDoS) attack on a kiosk machine and more

Furthermore, two additional job profiles from the ECSO minimum reference curriculum were used for the evaluations. We provide here the high-level description of these job profiles and refer to [ECSO21] for further details.

Enterprise Cybersecurity Practitioner: This practitioner masters risk management from a cybersecurity perspective. They should understand at least superficially the company's network architecture and security vulnerabilities, including storage and computation facilities. They can assess the risks and choose measures to mitigate them, e.g. advising on the best solutions for the company: for mobile devices, cloud storage and computation, cryptographic techniques, response team size and composition, etc.

Cybersecurity Analyst: This profile is proficient with network administration (including security), e.g. for architecture and vulnerability analysis, also threat identification and mitigation. A cybersecurity analyst should be at least moderately proficient in cyber incidents response, such as performing a penetration analysis using professional tools.

3.1.2 Conclusions from the evaluations

In Annex A, we provide the skills evaluations for the aforementioned six long-term job profiles. 14 evaluations were made by professionals of various fields of cybersecurity in six different organisations. The countries represented were Denmark, Finland, Italy, Slovenia and Spain. In Table 13 in Annex A, we show the evaluation results for the six job profiles. The skills with the highest demand across all profiles are displayed in Table 7, by the average value of each skill (with a scale from 0 to 3).

Table 7: Cybersecurity skills with the highest average demand.

Skill	Demand (0–3)
Risk Management	2.21
Network Defence	2.16
Business Continuity, Disaster Recovery, and Incident Management	1.96
Network Architecture	1.90
System Control	1.90
Access Control	1.89
Secure Communication Protocols	1.87
Common System Architectures	1.84

Security Governance & Policy	1.82

Similarly, in Table 8 we summarise the skills with the lowest demand across the profiles:

Table 8: Cybersecurity skills with the lowest average demand.

Skill	Demand (0–3)
Awareness and Understanding	1,10
Design	1,09
Component Design	1,08
Social and Behavioural Privacy	1,08
Physical Media	1,05
Physical Interfaces and Connectors	1,05
Component Reverse Engineering	1,01
Ethics	0,93
Component Procurement	0,64
Customer Services and Technical Support	0,49

3.2 Integrating research and innovation

Education programs shall continuously monitor and integrate state-of-the-art research and innovation to keep training up-to-date and relevant. In that respect, this section provides concrete examples taken from the research (WP3) and innovation (WP5) work packages of CyberSec4Europe, that exemplify how today's state-of-the-art will affect the teaching curricula of cybersecurity in the following five to ten years. Table 9 and Table 10 indicate the most relevant knowledge areas for each research area and vertical sector of CyberSec4Europe. Annex D: Impact and Integration of Research and Innovation details the specific manner in which these areas are impacted by each demonstrator from WP5 or research initiative from WP3, including references to CyberSec4Europe deliverables where the relevant material is presented. Note that these tables merely serve to emphasise the most notable impact on each knowledge area but are not exhaustive.

Table 9: WP3 tasks and their involved knowledge areas.

Knowledge Area	Common Framework Design	Cybersecurity Enablers	Software Lifecycle	Security Intelligence	Adaptive Security	Usable Security	Regulatory Sources	Conformity and Certification	Continuous Scouting	Impact on Society
Data Sec.										
Software Sec.										
Component Sec.										
Connection Sec.										
System Sec.										
Human Sec.										
Org. Sec.										
Societal Sec.										
Op. and Maint.										

Table 10: WP5 tasks and their involved knowledge areas

Knowledge Area	Open Banking	Supply Chain	Privacy-preserving ID Mgmt.	Incident Reporting	Maritime Transport	Medical Data Exchange	Smart Cities
Data Sec.							
Software Sec.							
Component Sec.							
Connection Sec.							
System Sec.							
Human Sec.							
Org. Sec.							
Societal Sec.							
Op. and Maint.							

3.3 Beyond Traditional Education Formats

Future cybersecurity education will need to make use of contemporary teaching methods to maximise skill transfer potential. Due to the digital and continuously evolving nature of the field, it is especially suited for several new education formats that can work in conjunction with traditional formats to improve the learning experience and increase education quality.

In this Section, we summarise three modern education formats which have been investigated in the scope of this project. Firstly, we look at Massive Open Online Courses (MOOCs), which bring a traditional academic course format to the Web, open for anyone to enrol in. Afterwards, we look at cyber ranges, which let participants deal with real security challenges in realistic sandbox environments. Finally, we look at serious games, an engaging approach that allows players to learn useful security skills through a series of gamified challenges.

3.3.1 MOOCs

MOOCs have emerged over the last few years as an alternative to formal education, that also enables life-long learning for a broad group of students. The review of the current offer in cybersecurity MOOCs provided by [D6.1] stressed the need for regulatory enablers to foster open-learning recognition in EU Member States, especially for non-academic courses. For this purpose, CyberSec4Europe proposed quality assurance criteria for European MOOCs in [D6.1], which are both generic and cybersecurity-specific, and can both be used as a basis for evaluating and branding the quality of cybersecurity MOOCs in Europe.

In addition to general criteria that should apply for all types of MOOCs, specific criteria were defined for academic MOOCs issuing credit points for enrolled university students, continuous (life-long) learning MOOCs and future cyber range MOOCs. The criteria were derived from: (1) conclusions from a review of existing European MOOCs in terms of gaps to be addressed, (2) regulations and ethical standards, (3) criteria taken from existing quality assurance frameworks, including [Brits16,RJ14,ST18], and (4) existing best practices and our experiences — see [FBL+20].

Below, we list the main categories of the quality criteria and summarise their main requirements[1]:

QC1 - Qualification of the Proposer: The proposing institution ("proposer") should have the proper qualification and experience to be able to develop, run and evaluate the MOOC in a professional manner, and be recognised by the cybersecurity community. For cyber range MOOCs, the proposer's cyber range should be technical, work-life oriented which can mimic realistic phenomena (e.g. attack campaigns, threat actors, techniques, tools, etc.) from the cybersecurity field.

QC2 - Qualification of Participants: The admission criteria and process must be fair and transparent. The participants must have the qualifications needed for taking the MOOC. For cyber range MOOCs, the participants should have the skills to operate a technical cyber range platform, unless this is taught in the course.

QC3 - Qualification of Instructors: The instructors must have an academic degree and/or teaching experience and should have a pedagogical education. For cyber range MOOCs, at least one of the instructors should have the technical skills required for conducting and supervising all operations.

[1] The modal verbs used in the QCs reflect the existence—or lack thereof—of legal requirements for the affected parties. For example in QC2 and QC3, "must" indicates the presence of strong regulations: the participants *must have* the qualifications needed for taking the MOOC; and the instructors *must have* an academic degree and/or teaching experience. In contrast in QC1, the proposing institution *should have* the proper qualifications: this indicates that it is still legally permissible for an institution to provide MOOCs, despite not having formal qualifications for it.

QC4 - Examination and Credentialisation: For awarding credits or certificates, the examination has to verify that learning goals have been achieved in a transparent manner. Therefore, any cyber range activities, laboratory work, and assignment that is mandatory for obtaining a course credential should be clearly stated. Course certificates should always be issued for recognition of the educational achievements in the professional or life-long/blended learning context. Academic European MOOCs should be recognised as a valid credit-awarding course within the European credit transfer system.

QC5 - Course Evaluations: Means for continuous course evaluations implemented by participants should be in place.

QC6 - Meeting Professional Expectations: Suitable stakeholders, especially from working life and the employment side, should be involved throughout the MOOC development and operation. When providing a cyber range course to a company or an organisation, it should be "realistic enough", i.e. simulate operational and supporting services and systems available for the participants.

QC7 - Course Structure, Content and Evaluation: The MOOC should provide an overview presenting its goals and structure, the main content, format, reference literature, language, knowledge and skills as prerequisites, as well as the learning outcome to be acquired. The MOOC should cater for different learning styles and strategies to reach the learning outcomes. Proposers should review the MOOC and its content periodically, so that the content reflects the state of the art and continues to fulfil its learning goals.

QC8 - Course Platform and Channels: Only platforms and channels that comply with the EU General Data Protection Regulation (GDPR) must be selected. Moreover, the functionality of the platform should comply with the EU Directive 2016/2102 on the accessibility of the websites and mobile applications of public sector bodies for ensuring inclusiveness.

QC9 - Openness: Openness should be guaranteed both in terms of the MOOC content and material (by using open licensing, e.g. CC-BY-SA, allowing to freely reuse, mix and redistribute material), as in terms of being open and adapting to the learner's needs, enabling them to study at any time, place and pace of choice. There should be clear, transparent and justifiable policies for defining any restrictions to digital openness (e.g. for the use of malicious or attack code for teaching purposes) and/or openness of course elements (e.g. those that are hacking-related or for other reason security-sensitive) to learners for ethical or security reasons.

QC10 - Ethics: Cybersecurity MOOCs should due to the sensitivity of the subject (methods of attacks, exploitation of vulnerabilities, implementation of measures) introduce and enforce ethical principles for cybersecurity courses in regard to ethical hacking, handling security-sensitive information and personal data.

QC11 - Privacy: The MOOC owner having the role of the data controller must ensure that all personal data of the participants of the course, as well as the instructors, are processed in compliance with the GDPR and other applicable laws. Especially, the platform and course instances storing personal data must be secured by appropriate security controls and should follow the privacy by design and by default principle (Art. 25 GDPR).

QC12 - Utilising Cyber Ranges: The proposer's cyber range should provide systems and services for planning, running and doing post-exercise analysis and for allowing the defending team to prevent, detect, mitigate and recover from cyber incidents.

Validation study: a survey has been conducted to allow a direct assessment of these quality criteria by the cybersecurity community [BCF21]. The survey, consisting of 72 questions, was completed by 86 people from over 15 EU countries. Respondents vary in age (18–24: 3%, 25–44: 65%, 45–65: 29%, 65+: 2%), role (educator: 40%, employee: 26%, MOOC instructor: 10%, student: 10%, employer: 8%, other: 6%), and gender (female: 33%, male: 62%, abstain: 6%). Results show an active interest and need for MOOC certification, and a large agreement by respondents to achieve this using the quality criteria

QC1–QC12 detailed above. In particular, the majority of respondents would value a MOOC certificate that shows that a MOOC fulfils specific acknowledged criteria, which should have been reviewed by an institution independent from the proposer.

Later in the document, Section 4.1 will explain how the quality criteria were used to evaluate MOOC offerings, while Section 4.2 will explain how quality criteria were evaluated by MOOC stakeholders.

3.3.2 Cyber Ranges

Cybersecurity is instrumental for the business continuity of an organisation and its ecosystem, but it is often not important *per se*: it is a means to maintain the integrity of the company's data and cyber assets. Achieving the required degree of security typically calls for special training in areas that may lie outside the main scope of the organisation. To this aim, cyber ranges offer an effective hands-on cybersecurity learning experience that can be integrated and run within organisations.

Within CyberSec4Europe we have successfully conducted two cyber ranges [D6.4. D6.5], internally called "Flagship cybersecurity exercises". Both exercises, and in particular the open analyst activity introduced in Flagship 2, support fulfilling the current cybersecurity skills, knowledge and abilities (KSA) demand of European private companies and public organisations. They can be adapted to training: for example they were scheduled to last two business days, and with modifications it might be possible to execute the exercises in one business day.

The Flagship exercises can be used to train the participants working in a situation where a cybersecurity incident has happened. In **Flagship 1** the participants could use either the pre-created incident response plans, which had purposefully-introduced gaps, or an organisation could use its existing plans and apply them to the situation. After the exercise debriefing, the organisation should improve the gaps detected in the plan. Flagship 1 had roles for top management, and specialists of communication, law (GDPR), IT and cybersecurity. Thus the exercise emulated a realistic cybersecurity environment, where technical roles operate with e.g. managerial and legal personnel. In our experience, including such non-IT roles covers interaction aspects—crucial for a business perspective—that cannot be deployed with technical roles alone. In an educational context the learners could create the incident response plans and apply them in the exercise whilst simulating an organisation.

The **Flagship 2** exercise was more technical in nature. The participants detected a cybersecurity incident to which they (technically) responded and mitigated within a simulated Internet, offered via an ISP created for that purpose. The environment contained a trackside network with a full-stack simulated environment from radio block centres down to the level of train firmware, which participants needed to analyse to discover the information and systems that had been compromised. Technically-oriented cyber ranges demand such a degree of low-level implementation, which can bloat its preparation time when implemented for the first time. The counterpart is that incident response will be highly increased during subsequent real attacks.

To allow for fully independent operation, the participants would require several days of practice in the environment prior to the exercise. To remove this need, the Flagship exercise participants had a coach, who provided guidance when needed on how to use the systems and security controls. In the education context the learners could familiarise themselves with the learning environment, before the exercise began, to gain practice, although no objective was set to *learn* the system operation. We note that in a business or organisational (training) context that is not always possible due to time constraints, which must be taken into account when using our experience reports to design new cyber ranges.

The detailed story line and objectives were not revealed to the participants before the exercises, simulating real-life situations. An attacker rarely, if ever, informs the target organisation about the forthcoming attack or the attacker's objectives. In the self-paced learning context, these should be opened to the participants, so they can follow the tracks by themselves. For self-paced learning the exercise contents should be tested with one or two groups to verify that the attacker trails can be found

and that there are no gaps in the attacker's story-line.The suggested way to deploy such courses is via an iterative control loop, where feedback from the first participants is used to improve the experience of the second course and so on. The nature of the feedback collected should be aligned with the course objectives, and defined prior to starting the exercise. During the exercise, the participants could be assessed by technically monitoring their work and performance, or by using a learning management system or a capture the flag platform where participants submit the candidate flags (like analysts did in the analyst activity) and the system checks if the submitted flag is correct for the challenge (task), or by some other means.

The open analyst activity in Flagship 2 was an entry-level digital forensic activity. Technically it was a variant of a capture-the-flag event with no positive or negative scoring of participants. This learning experience is expected to be well-suited to workforce training with minor guideline modifications. It could be used for assessing a work candidate's skills and abilities in digital forensics. It could also be used for self-paced training of career changers, e.g. from technical IT or software development to technical cybersecurity. Assessing the learning could be done by comparing the number of flags found and the time spent resolving the challenges, or by some other means.

3.3.3 Serious Games

Many traditional security training programs mostly fail in imparting and consolidating knowledge because of the following reasons[2]:

1. They are perceived as a work obligation, failing to stimulate the personal interest in behavioural change.
2. They do not offer customisation, proposing a single progression rate, regardless of differences between users.
3. They are concentrated in fixed and rare moments (e.g. twice a year) and forgotten as time passes.

To stimulate interest, repetition and change of habit, a promising approach experimented with for many years now is the use of games as vehicles of knowledge diffusion. This concept is known as Serious Games (SGs); these are "games", (i.e. activities that generate fun and catch interest) with a "serious" purpose, i.e. to transmit and practice knowledge. In Security Serious Games (SSGs) the knowledge to be spread relates to cybersecurity.

SSGs are attractive educational tools: according to cognitive research, the attention paid during a lecture may start to decrease after 10-20 minutes [Brad16], while a player can stay focused on a game even for hours. In detail, the "fun" aspect may keep the player engaged, the "discovery" aspect may keep the player interested and involved in the story, with the curiosity to explore the virtual world, and the "challenge" aspect may give the player a sense of accomplishment to surpass obstacles in the course toward the goals. All these aspects motivate a player and need to be sustained through feedback responses, reflection, and active involvement for designed learning to take place [GAD02]. Therefore the key challenge for effective learning with games is for the learner to be engaged, motivated, supported, and interested [PRE01, BCD89].

Since 2002, serious games have increasingly become more acknowledged as a valid learning tool. Today serious games are widely used for military, health personnel, and corporate training as well as to teach people about various subjects such as science [ETE11, MIL09, KRK+12], economics [GF94, VIR06, BTG+16], politics [DEM05, DEM07, PEO, DAR07, MER20], and cybersecurity as well. Examples of SSGs include CyberCIEGE [ITA05, TI14], the Agent Surefire series [MAV], and Anti-Phishing Phil

[2] Based on a study published by the SANS institute [Spi19], in turn based on NIST's (SP800-50) and ENISA's guidelines for planning and deploying security education.

[SBP+07]. In Annex C: Serious Games a more comprehensive list of cybersecurity games is included, together with a description briefly indicating their characteristics.

Analysing some of the most notable SSGs, five key aspects to emphasise are:

- Allow the users to impersonate an attractive role (e.g. a secret agent capable of arresting cyber criminals, the head of a security department in a company, etc). Moreover, provide a plot to excite the users with the story at hand, which at the same time allows them to create a mental connection with real stories.
- Balance the game progression, allowing a user to not get frustrated (because of difficulty) or bored (when it stays too easy)
- Track the progress to measure the evolution, typically by embedding logging capabilities in the game engines, and sometimes also allowing custom log development for custom scenarios (e.g. cyberCIEGE, which is developed for enterprise training)
- Provide representations or metaphors closely related to real situations, allowing users to contextualise game scenarios with real-world cases.
- Identify a target audience and be consistent with it, e.g. very different games and assumptions can be made if the target player is a medium computer user that needs some security awareness training, or if instead it is a security expert that needs to understand some new security mechanisms.

SSGs are particularly suitable to mitigate the vulnerability of the human factor by raising awareness of security issues and solutions and improving the technical knowledge, and in some cases, they can be an effective means of evaluation of the user's security knowledgeEducation Assessment Framework

4 Education Assessment Framework

This section answers the question "How does one assess and evaluate the quality of an education offer?". For that, we first summarise in Section 4.1 our quality-criteria based approach to evaluating single education units offered as MOOCs. We then report in Section 4.2 on an online survey that we conducted to analyse the role of cybersecurity MOOC certification based on the proposed quality criteria for cybersecurity. Last, Section 4.3 presents a quality branding process for cybersecurity MOOCs.

4.1 Education Unit Assessment

CyberSec4Europe conducted an exemplary evaluation of selected cyber security MOOCs in [D6.1] by applying a subset of the defined quality criteria described in The CyberSec4Europe Knowledge Framework, with a focus on criteria that are specific to cybersecurity.

Four academic MOOCs and two continuous learning MOOCs were evaluated. Our evaluation procedure had three phases and implemented a peer review process, which was mandatory for evaluating criteria that were subjective and potentially open for interpretation like QC9: "*Assessment methods must be aligned with the learning objectives and be measured by valid means"*.

In the first phase, each MOOC was independently evaluated by five or six project partners. In the second phase, these five to six evaluation lists were collected and combined into a single document. In the third phase, in case of deviating ratings for criteria, a consensus discussion among involved partners took place.

Ratings and Openness of Information: Our evaluation exercise showed that not all information for evaluating the quality of MOOCs is openly available. This is illustrated in Table 11, which shows the average percentages of unclear ratings due to a lack of available information for different categories of criteria.

Information about the proposing institute was rather visibly published. Also, information needed to evaluate the course examination, credentialization, and recognition criteria as well as the course structure and content criteria were mostly available online.

Ethical considerations for teaching cyber security, including ethical rules for students for handling security-sensitive information, were only clearly addressed for a quarter of the analysed courses.

On average only a third of the privacy criteria were clearly fulfilled. In particular, only a small fraction (37%) of the evaluated MOOCs has a clear policy statement specifying how student-performance data collected by the course platforms are used by the course owners.

Finally it is also notable that criteria about meeting professional expectations were on average only clearly fulfilled in less than 15%. In particular, many of the courses failed to involve cyber security stakeholders in the course design, implementation, realisation, and/or periodic review.

Table 11: Average distribution of criteria assessment ratings per criteria category for the evaluated MOOCS in percentages.

Category of Criteria	yes	partly	no	unclear
Qualification of the proposing institution	80.5	2.4	12.2	4.9
Course structure and content criteria	55.2	12.8	3.2	28.8
Qualification of instructors	52.8	8.3	2.8	36.1
Course examination, credentialization, and recognition	40.6	4.2	32.3	22.9
Privacy requirements	37.1	8.6	14.3	40.0
Openness	33.3	0.0	0.0	66.7
Ethical considerations for teaching cybersecurity	25.0	4.2	20.8	50.0
Meeting professional expectation	14.3	0.0	21.4	64.3
Average	45.2	7.0	14.7	33.1

Implications for a Quality Seal Awarding Process. The three-phase evaluation process consisted of independent evaluation by several experts, consolidation, and moderated consensus discussions and decisions. All participants agreed that the final results were meaningful and the process worked well and efficiently, and is thus recommended as part of a governance structure for awarding the quality seal to MOOCs by a European Cyber Security Competence Network. This is reported in [FBL+20] and briefly discussed below in Section 4.3.

4.2 Survey on Certification

We conducted an online survey [BCF21] to analyse the role of cybersecurity MOOC certification based on proposed quality criteria for cybersecurity MOOCs and for MOOCs in general presented in Education Unit Assessment. Participants reported mixed experiences with MOOCs and largely agreed with our proposed quality criteria.

The survey consists of 72 questions in total. Some of the main questions are conditional, i.e. questions about MOOC experiences are only asked if the participant participated in at least one MOOC before. Accordingly, questions about cybersecurity MOOCs are only asked if the survey participant had attended at least one cybersecurity MOOC. An overview of the survey questions can be seen in Table 12.

Table 12: Categories of questions.

Part	n	Scale	Topic
Demographics	8	mixed	Demographic Information
Part A	11	Quantitative	Former experiences with MOOCs
Part B	5	Likert	Criteria that factor in the selection of a specific MOOC
Part C	6	Likert	Which are the statements or properties that should be conveyed by a MOOC certificate?
Part D1	20	Quantitative	Challenges encountered by the participants during their MOOC experience. Five of the questions are specific to Cybersecurity MOOCs and appear when such a participation is confirmed
Part D2	20	Likert	Quality aspects that should be included in a (Cybersecurity) MOOC Certification for addressing these challenges?
Part E1	1	Text	Other challenges (optional); What other challenges could be addressed by a relevant certification scheme?
Part E2	1	Text	Email address (optional - for being contacted for further feedback)

The surveyed MOOC stakeholders largely agreed with the quality criteria proposed. Our results suggest that there is not only high acceptance of the quality criteria, but also an interest and need for MOOC certification.

The instructor and *quality rankings by other users* were agreed by most MOOC stakeholders as a main factor in the selection of a MOOC. A majority (72%) also sees a MOOC certificate as a selection factor. Also the fact that 81% of our participants are considering the quality rankings by other users shows us that there is a need for information about the quality of MOOCs. User ratings can however be quite easily manipulated, which is a clear argument for the need of an official certification process.

Non-educators agreed — even slightly more often than educators — that the instructor should be factored in when selecting MOOCs. Hence, we noticed no obvious bias by educators overestimating their importance. These results also indicate that quality criteria for the qualification of the instructor should play an important role in a certification scheme, although the exact way this could be factored in is still an open issue.

Only 26 out of 56 MOOC stakeholders answered the two openness-related questions D1.11 and D1.12, whereas all other questions about general experiences in MOOCs were answered by at least 53 participants. One possible explanation could be that those who skipped the question were not sure if

their MOOCs were lacking in openness, as they may not need accessibility features themselves and therefore did not perceive it as a challenge directly. This should be kept in mind when observing that 43% of those who answered the relevant questions reported accessibility issues.

The fact that *privacy of MOOC platforms* was encountered as a major challenge does not come as a surprise given that most of the leading MOOC platforms are hosted by non-EU providers. This means that data about the MOOC participants including sensitive information about their course performance and activities may flow to a third country outside the EU without adequate data protection and thus in noncompliance with the GDPR.

Therefore, privacy including GDPR compliance can be seen as an important quality criteria for a European cybersecurity MOOC certification scheme.

The survey [BCF21] results also help answering our research questions as described below:

RQ1: **How do (cybersecurity) MOOC stakeholders value a certificate as a selection criteria and what should such a certificate convey?**
Answers to Part B of the survey showed that a majority of the MOOC stakeholders (both educators and non-educators) value a MOOC certificate showing that a MOOC was independently reviewed and fulfils specific acknowledged criteria, and agreed using it as a factor for selecting a MOOC. Moreover, the majority of survey participants chooses that all suggested quality aspects in Part C should be conveyed by a certification scheme.

RQ2: **What challenges have current (cybersecurity) MOOC stakeholders experienced?**
Answers to Part D1 of the questionnaire reveal that all challenges in the questionnaire were also experienced by at least some of the MOOC stakeholders. Most of the experienced challenges that were reported are related to privacy, accessibility, and openness. However, issues concerning the instructors' qualification, the quality of the proposer, undefined learning goals, or learning goals not aligned with the examination were also experienced by many stakeholders.

RQ3: **What quality criteria do stakeholders want to be included in a certification scheme for addressing such challenges?**
Our survey participants largely agreed that the quality criteria in Part D2 should be included in a certification scheme to address the highlighted challenges. The respondents (educators and non-educators) generally agreed that the proposed criteria should be included in a certification scheme for cybersecurity MOOCs, while also providing some prioritisation information (e.g. D2.7: the quality of material vs. D2.4: the self-assessment ability). Further analysis needs to be done to weigh the relevant criteria against the best practices and decide on the final set. Finally, the actual criteria and the structure of the certification scheme will be derived also taking into consideration the points mentioned in Education Unit Assessment, the concerns raised by the open questions and the results of the further analysis.

4.3 Assessing Education Governance

Based on our quality criteria, a quality branding process for cybersecurity MOOCs was defined and tested in a field study based on an exemplary evaluation that the CyberSec4Europe project conducted internally [FBL+20, D6.1]. The proposed process consists of the following eight steps that are also shown in Figure 3.

Step 1 – Application for quality branding: The institution seeking a quality branding submits its application, including documentation demonstrating how quality criteria have been met by them, when they submit their application for a quality branding.

Step 2 – Assessable criteria evaluation: All criteria that can be objectively assessed are evaluated. These are criteria that are measurable by a third party, and/or are fulfilled if there is a (required) official legal document or internal policy document.

Step 3 – Peer-review of criteria: All remaining subjective quality criteria are evaluated by a group of at least 3 experts in a peer-review process. In this peer-review process, the experts first assess the fulfilment of the criteria independently based on their expertise and experiences. Then a discussion of all reviews takes place among the experts followed by a moderated consensus meeting for agreeing on an assessment and decision. If all criteria are fulfilled, step 6 follows next.

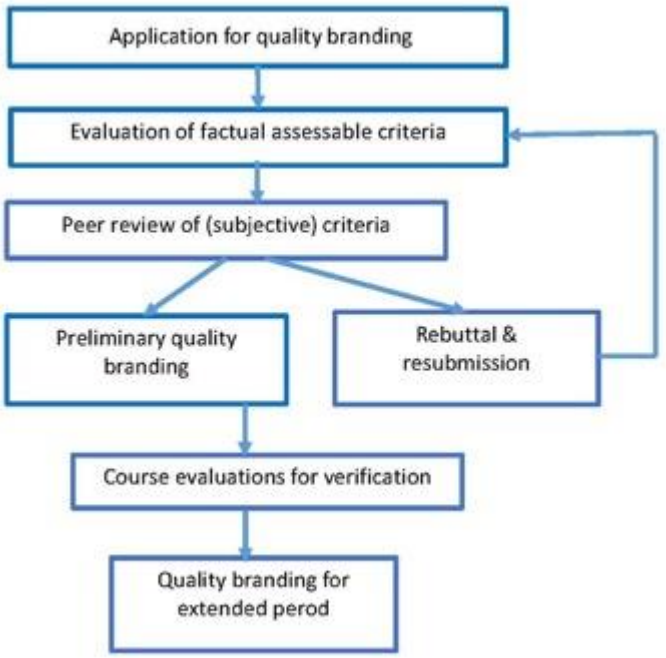

Figure 3. The proposed education governance process

Step 4 – Rebuttal and resubmission phase: Only MOOCs that clearly fulfil all quality criteria that are not formulated as optional should be quality branded. For any non-optional criteria that are not met, partly met or that are unclear, the proposer should be requested to address these open issues first and then resubmit the application for a quality branding.

Repeat step 2-4: Upon resubmission, steps 2 to 4 are repeated.

Step 5 – Preliminary Quality branding for first-time MOOCs: Ultimately, active participation in a MOOC might be needed to reliably retrieve all information needed for the evaluation. Even creating an account and subscribing to a course often does not provide all information needed, since some MOOCs are not active at the moment of review and the related information is not (yet) retrievable. If a MOOC runs for the first time, a preliminary assessment and quality branding should be given that is re-evaluated after the first iteration of the MOOC is completed.

Step 6 – MOOC evaluation by course participants for verification: Any preliminary quality branding evaluation is complemented by gathering feedback from students that participated in the MOOC. If the course evaluations reveal issues in regard to the practical fulfilment of the quality criteria, these issues need to be addressed and re-evaluated through step 2–4 before the period for the quality branding can be extended.

Step 7 – Quality branding for an extended time period: If all quality criteria are met for a MOOC that has been successfully given at least once, a quality branding is awarded for a longer time period. It is important to decide how often a provided quality branding should be reevaluated, since MOOCs are naturally subject to changes and may get outdated. Ideally, a revaluation should happen after each iteration of a MOOC for considering any changes — nevertheless, the costs and time for re-evaluations need to be considered as well, to decide on the optimal length of the period. Hence, longer periods (e.g. 1–3 years) for the validity of quality brands may be appropriate.

5 Conclusion

The urgent need for education of highly-skilled engineers, scientists and other specialists in all areas of cybersecurity, calls for common guidelines and tools that support the design of capability building instruments, like the education and assessment framework developed within CyberSec4Europe that we have presented in this document. We highlight that the aim of the framework is *to provide effective guidelines and tools open to external sources and third-party material outside the consortium, including methodologies to ensure adequate quality standards*.

To this aim, the CyberSec4Europe Knowledge Framework [D6.2] provides a unifying structure and terminology for cybersecurity knowledge areas, topics and skills, intended to serve as solid common ground for designing and assessing education and training in cybersecurity, whichever its sector of application.

Such a framework can be used for several purposes, including the CyberSec4Europe methodology for cybersecurity skill evaluation methodology for job profiles initially presented in [D6.3], by allowing cybersecurity and domain experts to identify the relevant knowledge units of strategically-chosen job profiles—i.e. by determining how important those units are for the required skills of the profiles. Furthermore, to facilitate its use by European institutions, we have generated a correspondence between our framework and the ESCO standard, which we present in full in Annex B.

Cybersecurity is among the fastest moving fields in today's digital world, which means that education programmes must be continuously updated with state-of-the-art research and innovation knowledge to keep them up-to-date and relevant. For this purpose, and as a forward-thinking tool for the CyberSec4Europe framework, we have provided community-emergent suggestions on how to incorporate research and demonstrators (from CyberSec4Europe) into future educational offers. Moreover, we explain how non-traditional education formats such as cyber ranges, serious games and MOOCs can be used to offer suitable cybersecurity learning experiences.

Finally, to support quality assessment of educational offers (which our surveys have shown to be a main driver when students choose a course to follow), we present and discuss a quality-criteria-based approach to evaluating single education units offered as MOOCs, and a quality branding process for cybersecurity educational offers.

Overall, this deliverable provides an overview over most of the education and training activities that have been carried out within CyberSec4Europe. This includes curated summaries of key contributions presented in previous deliverables [D6.1, D6.2, D6.3, D6.4, D6.5], as well as novel contributions: Translations from our framework to the ESCO occupations and skills standard, guidelines to develop SSG and other gamification approaches to education, studies on job profiles of long prevalence in the cybersecurity field (border control), and incidence of current research initiatives into the knowledge areas defined in our framework.

6 References

[ACM17] CSEC2017 Joint Task Force. (2017, December 31). Cybersecurity Curricula 2017 — *Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. Retrieved from Association for Computing Machinery: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

[AGA+17] D.Antonioli, H.R. Ghaeini, S.Adepu, M.Ochoa, N.O.Tippenhauer (2017). Gamifying Education and Research on ICS Security: Design, Implementation and Results of S3. URL: https://arxiv.org/abs/1702.03067

[Atlas18] G. Hillenius (2018, January 30). Cybersecurity Atlas | EC to build partner network of cybersecurity experts. Retrieved from EUROPA - European Union website, the official EU website: https://joinup.ec.europa.eu/collection/egovernment/news/cybersecurity-atlas.

[BCD89] J. S. Brown, A. Collins, P. Duguid (1989). Situated Cognition and the Culture of Learning. In: *Educational Researcher*, Vol. 18 No. 1, pp. 32-42. DOI: 10.3102/0013189X018001032

[BTG+16] M. Beutner, M. Teine, M. Gebbe, L. M. Fortmann (2016). NetEnquiry--A Competitive Mobile Learning Approach for the Banking Sector. International Association for Development of the Information Society. URL: https://eric.ed.gov/?id=ED571446

[BCF21] M. Beckerle, A. Chatzopoulou, S. Fischer-Hübner (2021). Towards Cybersecurity MOOC Certification (under review).

[Brad16] N.A. Bradbury (2016). Attention span during lectures: 8 seconds, 10 minutes, or more?. In: *Advances in physiology education*, vol. 40.4, pp. 509-513. DOI:10.1152/advan.00109.2016

[Brits16] Commonwealth of Learning (2016). Guidelines for Quality Assurance and Accreditation of MOOCs. ISBN: 978-1-894975-82-7.

[CyBOK19] Rashid, A., Chivers, H., Danezis, G., Lupu, E., & Martin, A. (2019). CyBOK — The Cyber Security Body of Knowledge — Version 1.0. Retrieved from CyBOK: https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf.

[D3.1] A. Skarmeta (2020). D3.1: Common Framework Handbook I. Retrieved from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2020/06/D3.1-Handbook-v2.0-submitted-1.pdf

[D3.3] D. Preuveneers (2020). D3.3: Research Challenges and Requirements to Manage Digital Evidence. Retrieved from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2020/02/D3.3-Research-challenges-and-requirements-to-manage-digital-evidence-

Submitted.pdf

[D3.5] K. Halunen (2020). D3.5: Usable Security & Privacy Methods and Recommendations. Retrieved from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2020/02/D3.5-Usable-security-privacy-methods-and-recommendations-Submitted.pdf

[D3.6] B. Kežmah (2020). Guidelines for GDPR Compliant User Experience. Retrieved from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2021/02/D3.6-Guidelines-for-GDPR-compliant-user-experience-Revision-2.0.pdf

[D3.7] B. Crispo (2020). D3.7: Usability Requirements Validation. Retrieved from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2020/03/D3.7_Usability_requirements_validation_Submitted.pdf

[D3.8] L. Kamm (2020). D3.8: Framework and Toolset for Conformity. Retrieved from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2020/03/D3.8-Framework-and-Toolset-for-Conformity-v1.0-Submitted.pdf

[D3.9] A. Lluch Lafuente (2020). D3.9: Research Challenges and Requirements for Secure Software Development. Retrieved from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2020/09/CyberSec4Europe-D3.9-Research-challenges-and-requirements-for-secure-software-development-v1.1-Submitted.pdf

[D3.10] D. Canavese (2020). D3.10: Cybersecurity Outlook 1. Retrieved from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2021/01/D3.10-Cybersecurity-outlook-1-Submitted.pdf

[D3.12] A. Hita, A. Skarmeta (2021). D3.12: Common Framework Handbook 2. Retrieved from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2021/06/D3.12-Common-Framework-Handbook-2-v1.0-submitted.pdf

[D3.14] M. Guarascio, G. Manco (2021). D3.14: Cooperation With Threat Intelligence Services For Deploying Adaptive Honeypots. Retrieved from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2021/10/D3.14-Cooperation-with-Threat-Intelligence-Services-for-deploying-adaptive-honeypots_2.05_submitted.pdf

[D3.15] J. Resende (2021). D3.15: Proactive Approaches For Software Development. Retrieved from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2022/01/D3.15-Proactive-approaches-for-secure-software-development-v1.0_submitted.pdf

[D3.16] O. Latvala (2021). D3.16: Security Requirements And Risks Conceptualisation. Retrieved from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2022/01/D3.16-Security-requirements-and-risks-conceptualization-v1.0_submitted.pdf

[D3.18] B. Kežmah (2022). D3.18: Analysis Of Interoperability And Cross-Border Compliance Issues. Retrieved from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2022/04/D3.18-Analysis-of-interoperability-and-cross-border-compliance-issues-v1.0-Final_submitted.pdf

[D3.21] L. Pasquale (2022). D3.21 Framework to design and implement adaptive security systems. Retrieved from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2022/06/D3.21-Framework-to-design-and-implement-adaptive-security-systems-v3.0-submitted.pdf

[D3.22] L. Kamm (2022). D3.22: Validation And Certification Methodology. Retrieved from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2022/06/D3.22-Validation-and-Certification-Methodology-v1.0_submitted.pdf

[D5.2] A. Sforzin (2020). D5.2: Specification and Set-up Demonstration case Phase 1. Retrieved from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2021/07/D5.2-Specification-and-Set-up-of-Demonstration-Case-Phase-1-v1.0_J-Submitted.pdf

[D5.5] A. Sforzin (2021). D5.5: Specification And Set-Up Demonstration Case Phase 2. Retrieved from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2022/01/D5.5-Specification-and-set-up-demonstration-case-Phase-2-v1.0_submitted.pdf

[D6.1] S. Fischer-Hübner (2019, July 31). D6.1: Case Pilot for WP2 Governance. — Deliverable D6.1 of CyberSec4Europe. Retrieved from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2020/06/D6.1-Case-Pilot-for-WP2-Governance-V4-.pdf

[D6.2] N. Dragoni, A. Lluch Lafuente, A. Schlichtkrull & L. Zhao (2020, January 31). D6.2: Education and Training Review — Deliverable D6.2 of CyberSec4Europe. Retrieved from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2020/02/D6.2-Education-and-Training-Review-V1.2-Submtted.pdf.

[D6.3] A. Karinsalo, K. Halunen (2021, January 31). D6.3: Design of Education and Professional Framework — Deliverable D6.3 of CyberSec4Europe. Retrieved from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2021/06/D6_3_Design-of-Education-and-Professional-Frame-work_Final.pdf.

[D6.4] J. Päijänen (2021, February 24). D6.4: Flagship 1 — Deliverable D6.4 of CyberSec4Eurpoe. Retrieved from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2021/06/D6.4-Flagship-1-v1.1-submitted.pdf

[D6.5] J. Päijänen (2022, April 12). D6.5: Flagship 2 — Deliverable D6.5 of CyberSec4Eurpoe. Retrieved from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2022/04/D6.5-Flagship-2-v1.3_submitted.pdf

[DAR07] Darfur is Dying (2007). Y8. URL https://www.y8.com/games/darfur_is_dying

[DEM05] Democracy 1 (2005). Positech.
URL: https://www.positech.co.uk/democracy/democracy1.html

[DEM07] Democracy 2 (2007). Positech. URL: https://www.positech.co.uk/democracy2/index.html

[ECSO21] WG5 PAPER - European Cybersecurity Education and Professional Training Minimum Reference Curriculum - SWG 5.2 (2021, November). Retrieved from European Cyber Security Organisation (ECSO): https://www.ecs-org.eu/documents/publications/61967913d3f81.pdf.

[ENISA19] The European Union Agency for Cybersecurity. (2019, December 10). Education map — ENISA. Retrieved from ENISA: https://www.enisa.europa.eu/topics/cybersecurity-education/cyberhead

[ETE11] EteRNA (2011). URL: https://www.eternagame.org/web/

[FBL+20] S. Fischer-Hübner, M. Beckerle, A. Lluch Lafuente, A. Ruiz Martínez, K. Saharinen, A. Skarmeta, P. Sterlini (2020). Quality Criteria for Cyber Security MOOCs. In: *WISE 2020*. IFIPAICT, vol. 579, pp. 46–60. DOI: 10.1007/978-3-030-59291-2_4.

[GAD02] R. Garris, R. Ahlers, J.E. Driskel (2002). Games, Motivation, and Learning: A Research and Practice Model. In: *Simulation & Gaming*, vol 33.4 pp. 441-467. DOI: 10.1177/1046878102238607

[GF94] J. S.Goodwin, S. G. Franklin (1994). The beer distribution game: using simulation to teach systems thinking. In: *Journal of Management Development*, Vol. 13 No. 8, pp. 7-15. DOI: 10.1108/02621719410071937

[GSV21] M. Gáliková, V. Švábenský, J. Vykopal (2021). Toward Guidelines for Designing Cybersecurity Serious Games. In: *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education (SIGCSE)*. DOI: 10.1145/3408877.3439568.

[MAV] MAVI Interactive, Agent Surefire.
URL: https://www.maviinteractive.com/products.html#agent-surefire

[IMM21] ImmersiveLabs (2021), Learning like hackers to stay ahead of the game. URL: https://www.immersivelabs.com/product/features/gamified/

[ITA05] C. E. Irvine, , M. F. Thompson, K. Allen (2005). CyberCIEGE: gaming for information assurance. In*: IEEE Security & Privacy*, Vol 3.3 pp. 61-64. DOI: 10.1109/MSP.2005.64.

[JRC19] Nai Fovino, I., Neisse, R., Hernandez Ramos, J., Polemi, N., Ruzzante, G.-L., Figwer, M., & Lazari, A. (2019). A Proposal for a European Cybersecurity Taxonomy. Retrieved from EUROPA - European Union website, the official EU website: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf.

[KRK+12] A. Kawrykow, G. Roumanis, A. Kam, D. Kwak, C. Leung, C. Wu, E. Zarour, Phylo Players, L. Sarmenta, M. Blanchette, J. Waldispühl (2012). Phylo: A Citizen Science Approach for Improving Multiple Sequence Alignment. PLoS ONE. DOI: 10.1371/journal.pone.0031362

[MER20] Merchants (2020). ARC Institute.
URL: https://arc-institute.com/en/serious-business-games-2/merchants

[MIL09] C. Milburn (2009). Digital Matters: Video Games and the Cultural Transcoding of Nanotechnology. In: *Governing Future Technologies: Nanotechnology and the Rise of an Assessment Regime*, Springer. pp. 121–4. ISBN: 978-90-481-2833-4

[NIST17] Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017, August). NIST Special Publication 800-181 — National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Retrieved from National Institute of Standards and Technology | NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

[NIST20] Petersen, R., Santos, D., Smith, M.C., Wetzel, K.A., & Witte, G. (2020). NIST Special Publication 800-181, Revision 1 — Workforce Framework for Cybersecurity (NICE). Published by the National Institute of Standards and Technology (NIST). DOI: 10.6028/NIST.SP.800-181r1.

[PEO] People Power. Games For Change.
URL: https://www.gamesforchange.org/games

[PRE01] M. Prensky, (2001). Fun, Play and Games: What Makes Games Engaging. In: *Digital Game-Based Learning*, McGraw-Hill, California. pp. 05-1-05-31, ISBN: 0071363440. URL: http://www.autzones.com/din6000/textes/semaine13/Prensky%282001%29.pdf

[RJ14] J. Rosewell & D. Jansen (2014). The OpenupEd quality label: benchmarks for MOOCs. International Journal for Innovation and Quality in Learning, 2(3), pp. 88–100. URL: https://www.openuped.eu/images/docs/OpenupEd_Q-label_for_MOOCs_INNOQUAL-160-587-1-PB.pdf

[SBP+07] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, E. Nunge (2005). Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In: *Proceedings of the 3rd symposium on Usable privacy and security*, SOUPS' 07. pp 88-99. DOI: 10.1145/1280680.1280692

[Spi19] L. Spitzner (2019). Top 3 Reasons Security Awareness Training Fails. SANS Institute. URL: https://www.sans.org/blog/top-3-reasons-security-awareness-training-fails/

[ST18] C.M. Stracke & E. Tan (2018). The Quality of Open Online Learning and Education: Towards a Quality Reference Framework for MOOCs. In: *ICLS 2018*, pp. 1029–1032. URI: http://hdl.handle.net/1820/9909

[TI14] M.F. Thompson, C. E. Irvine (2014). CyberCIEGE scenario design and implementation. In: *USENIX Summit on Gaming, Games, and Gamification in Security Education*, 3GSE 14. 2014. URL: https://www.usenix.org/system/files/conference/3gse14/3gse14-thompson.pdf

[VIR06] Virtonomics, URL: https://virtonomics.com/

Annex A: Job Profile Assessment

Table 13 presents an extended use of the CyberSec4Europe Assessment Framework [D6.3], by evaluating job profiles expected to be relevant in the long term in the field of cybersecurity in Europe. Equivalently to [D6.3], here each job profile is evaluated on a scale 0-3 according to the skill level required in the profile work, in which 0 means "no skill required" and 3 means "advanced knowledge/skill required". Job profiles 1-4 consist of the ones defined in the "Use Case Border Control Intra EU" and the related scenario described in Section 3.1, namely:

1. General Cybersecurity Auditor
2. Technical Cybersecurity Auditor
3. Threat Modelling Engineer
4. Security Engineer
5. Security Engineer
6. Enterprise Cybersecurity Practitioner

The additional two job profiles (5 and 6) represent professions directly related to items listed in the Minimum Reference Curricula presented by ECSO in 2021[ECSO21]:

In total, 14 professional evaluations were done to construct the values. The evaluators represent project organisations and their stakeholders from Finland, Denmark, Slovenia, and Italy. Later, further studies were conducted — and are currently under analysis — to have this extension also assessed by CyberSec4Europe partners from Spain, Greece, Hungary, the Czech Republic, Germany, Estonia, and Norway.

Table 13: Evaluation results for skills required in cybersecurity long-term job profiles

		Job Profile (1–6)					
	Skill	***1***	***2***	***3***	***4***	***5***	***6***
Data Security	Cryptography	1.08	1.62	1.23	1.77	1.42	1.67
	Digital Forensics	1.15	1.69	1.69	2.08	1.00	2.17
	Data Integrity and Authentication	1.62	2.15	1.46	2.08	1.75	1.58
	Access Control	2.07	2.08	1.62	2.00	1.83	1.75
	Secure Communication Protocols	1.62	2.15	1.54	2.00	1.92	2.00
	Cryptanalysis	1.00	1.69	1.15	1.54	0.83	1.25

	Data Privacy	2.15	2.00	1.38	1.77	1.42	1.33
	Information Storage Security	1.69	2.23	1.62	1.92	1.83	1.58
Software Security	Fundamental Principles	1.31	1.69	1.69	1.77	1.42	1.58
	Design	0.77	1.15	1.31	1.62	0.92	0.75
	Implementation	0.62	1.23	0.92	1.77	1.25	1.00
	Analysis and Testing	1.15	1.69	1.00	2.00	1.25	1.67
	Deployment and Maintenance	0.85	1.15	0.92	1.85	1.42	1.00
	Documentation	1.15	1.08	1.31	1.92	1.08	0.92
	Ethics	1.31	1.00	0.92	1.00	0.92	0.42
Component Security	Component Design	0.85	1.38	0.92	1.31	0.92	1.08
	Component Procurement	0.54	0.54	0.69	0.85	0.75	0.50
	Component Testing	1.00	1.62	1.00	1.77	0.75	1.50
	Component Reverse Engineering	0.69	1.31	0.85	1.31	0.67	1.25
Connection Security	Physical Media	0.54	1.38	0.85	1.38	1.17	1.00
	Physical Interfaces and Connectors	0.69	1.54	0.77	1.38	0.92	1.00
	Hardware Architecture	0.77	1.69	1.15	1.38	1.17	1.25
	Distributed Systems Architecture	1.00	1.77	1.31	1.92	2.00	1.92

	Network Architecture	1.31	2.08	1.46	2.15	2.17	2.25
	Network Implementations	0.85	1.69	1.15	2.31	2.17	2.08
	Network Services	1.15	1.54	1.23	2.08	1.83	1.67
	Network Defense	1.54	2.15	2.00	2.69	2.42	2.17
System Security	System Thinking	1.00	1.46	1.85	1.38	1.50	1.08
	System Management	1.62	1.62	1.85	2.00	1.58	1.25
	System Access	1.85	2.08	1.77	2.00	1.83	1.33
	System Control	1.85	2.08	2.08	1.92	2.08	1.42
	System Retirement	1.08	1.00	1.38	1.62	1.08	0.67
	System Testing	1.46	2.08	1.46	1.92	1.25	1.83
	Common System Architectures	1.46	1.77	1.69	1.85	2.33	1.92
Human Security	Identity Management	1.85	1.85	1.77	1.62	1.67	1.33
	Social Engineering	1.62	1.38	1.85	1.46	1.50	1.92
	Personal Compliance with Cyber Security Rules/Policy/ Ethical Norms	1.85	1.54	1.46	1.69	1.50	1.25
	Awareness and Understanding	1.15	0.92	1.15	1.23	1.33	0.83
	Social and Behavioral Privacy	1.23	1.00	1.08	1.15	1.25	0.75
	Personal Data Privacy and Security	1.85	1.54	1.46	1.62	1.50	1.42

	Usable Security and Privacy	1.54	1.31	1.23	1.46	1.25	1.17
Organisational Security	Risk Management	2.46	2.15	2.54	1.69	2.67	1.75
	Security Governance & Policy	2.23	1.38	1.85	1.85	2.17	1.42
	Analytical Tools	1.92	2.08	1.31	1.69	1.75	2.08
	Systems Administration	1.92	1.85	1.38	1.54	1.75	1.25
	Cyber Security Planning	2.15	1.62	1.69	2.00	2.08	1.17
	Business Continuity, Disaster Recovery, and Incident Management	1.85	1.62	2.00	2.31	2.17	1.83
	Security Program Management	2.08	1.38	1.69	1.62	2.00	1.33
	Personnel Security	1.23	0.77	1.31	1.00	1.58	0.92
	Security Operations	1.54	1.23	1.31	1.77	1.75	1.17
Societal Security	Cybercrime	1.38	1.15	1.69	1.62	1.42	1.42
	Cyber Law	1.31	0.77	1.23	1.85	1.25	1.42
	Cyber Policy	1.46	0.85	1.38	1.54	1.17	1.25
	Privacy	1.62	1.46	1.31	1.23	1.42	1.33
Operate and Maintain	Customer Service and Technical Support	0.23	0.46	0.38	0.62	0.83	0.42

Annex B: ESCO Skills

Table 14 shows a mapping from job profiles and cybersecurity-related scenarios to the general classification recently presented to the EU by the classification of European Skills, Competences, Qualifications and Occupations (ESCO).

The cases considered here, one per row in Table 14, include the 12 job profiles previously presented in deliverable D6.3 [D6.3], plus the 4 new (long-term) job profiles presented in this deliverable in Section 3.1, plus the two profiles mapped from the ECSO Minimum Reference Curriculum.

The match between the profiles and the ESCO occupations was obtained by confronting the profiles' and the occupations' descriptions in terms of necessary knowledge and skills. More in detail, ESCO is the European classification of skills, competences and occupations; its aim is to define a "common language" on occupations and skills that can be used by different stakeholders in the different European countries in employment as well as education and training topics. ESCO has been chosen as it constitutes an emerging standard that some teaching institutions, e.g. the University of Murcia, are already consulting to plan their curricula.

As a final remark, we note that the columns for ESCO skills appear empty for the two legal profiles (Data Protection Lawyer and Cybersecurity for Lawyers). This is due to the fact that the ESCO skills connected to legal job profiles are specifically related to the legal field, and are thus not relevant for our analysis.

Table 14: ESCO job profiles related to each of the developed profiles or scenarios, and the connected essential and optional skills.

Profile/scenario	ESCO occupations	ESCO essential skills	ESCO optional skills
Data Protection Lawyer (DP)	Lawyer		
Security Certification Agent (SC)	ICT Security Consultant	analyse ICT system define security policies develop information security strategy educate on data confidentiality execute ICT audits execute software tests identify ICT security risks identify ICT system weaknesses implement ICT risk management manage IT security compliances manage disaster recovery plans perform risk analysis provide ICT consulting advice	lead disaster recovery exercises manage changes in ICT system optimize choice of ICT solution
Security Trainer (ST)	ICT Trainer ICT Security Administrator	apply company policies identify ICT system weaknesses maintain database security maintain ICT identity management manage IT security compliances perform ICT troubleshooting solve ICT system problems	address problems critically execute ICT audits execute software tests identify training needs lead disaster recovery exercises perform backups
Network Administrator (NA)	ICT Network Technician	implement ICT network diagnostic tools	migrate existing data perform ICT security testing
IoT Security Manager (IS)	ICT Security Manager	define security policies develop information security strategy	execute ICT audits identify ICT security risks

Profile/scenario	ESCO occupations	ESCO essential skills	ESCO optional skills
		establish an ICT security prevention plan implement ICT risk management lead disaster recovery exercises maintain ICT identity management manage disaster recovery plans manage IT security compliances solve ICT system problems	
Ensuring Integrity and Confidentiality 1 (IA)	ICT Security Manager ICT Security Administrator	apply company policies define security policies develop information security strategy establish an ICT security prevention plan identify ICT system weaknesses implement ICT risk management lead disaster recovery exercises maintain database security maintain ICT identity management manage disaster recovery plans manage IT security compliances perform ICT troubleshooting solve ICT system problems	address problems critically execute ICT audits execute software tests identify ICT security risks perform backups
Ensuring Integrity and Confidentiality 2 (IA)	ICT Security Manager ICT Security Administrator	apply company policies define security policies develop information security strategy establish an ICT security prevention plan identify ICT system weaknesses implement ICT risk management lead disaster recovery exercises maintain database security maintain ICT identity management manage disaster recovery plans manage IT security compliances perform ICT troubleshooting solve ICT system problems	address problems critically execute ICT audits execute software tests identify ICT security risks perform backups
Ensuring Integrity and Confidentiality 3 (IA)	ICT Security Manager ICT Security Administrator ICT Disaster Recovery Analyst	apply company policies conduct impact evaluation of ICT processes on business define security policies develop information security strategy establish an ICT security prevention plan identify ICT security risks identify ICT system weaknesses implement ICT recovery system implement ICT risk management lead disaster recovery exercises maintain database security maintain ICT identity management maintain plan for continuity of operations manage disaster recovery plans manage IT security compliances manage system security optimise choice of ICT solution perform backups perform ICT troubleshooting	address problems critically execute ICT audits execute software tests

Profile/scenario	ESCO occupations	ESCO essential skills	ESCO optional skills
		solve ICT system problems	
Ensuring Legitimate Access (CL)	ICT Security Administrator	apply company policies identify ICT system weaknesses maintain database security maintain ICT identity management manage IT security compliances perform ICT troubleshooting solve ICT system problems	address problems critically execute ICT audits execute software tests lead disaster recovery exercises perform backups
Security Intelligence (SI)	ICT System Administrator	administer ICT system apply ICT system usage policies implement ICT recovery system manage changes in ICT system manage system security manage system testing migrate existing data perform backups solve ICT system problems	implement ICT risk management
Cross-Border Authentication (CB)	Chief ICT Security Officer	ensure adherence to organisational ICT standards ensure compliance with legal requirements ensure information privacy implement ICT risk management lead disaster recovery exercises maintain plan for continuity of operations manage disaster recovery plans manage IT security compliances	optimise choice of ICT solution
Cyber Security for Lawyers (CS)	Lawyer		
General Cybersecurity Auditor	ICT Auditor	analyse ICT system execute ICT audits perform security vulnerability assessments	apply information security policies identify ICT security risks identify legal requirements manage IT security compliances
Technical Cybersecurity Auditor	ICT Auditor Manager	ensure adherence to organisational ICT standards ensure compliance with legal requirements execute ICT audits identify legal requirements implement ICT risk management manage IT security compliances	develop ICT test suite develop information security strategy ensure information privacy manage changes in ICT system
Threat Model Engineer	ICT Security Manager	define security policies develop information security strategy establish an ICT security prevention plan implement ICT risk management lead disaster recovery exercises maintain ICT identity management manage disaster recovery plans manage IT security compliances solve ICT system problems	execute ICT audits identify ICT security risks
Security Engineer	ICT Security Technician	address problems critically analyse ICT system	comply with legal regulations execute ICT audits

Profile/scenario	ESCO occupations	ESCO essential skills	ESCO optional skills
		execute software tests identify ICT system weaknesses manage alarm system solve ICT system problems use access control software	manage IT security compliances
Enterprise Cybersecurity Practitioner	ICT Security Consultant Chief ICT Security Officer	analyse ICT system define security policies develop information security strategy educate on data confidentiality ensure adherence to organisational ICT standards ensure compliance with legal requirements ensure information privacy execute ICT audits execute software tests identify ICT security risks identify ICT system weaknesses implement ICT risk management lead disaster recovery exercises maintain plan for continuity of operations manage IT security compliances manage disaster recovery plans perform risk analysis provide ICT consulting advice	manage changes in ICT system optimise choice of ICT solution
Cybersecurity Analyst	ICT Security Technician ICT System Analyst ICT Network Technician	address problems critically analyse ICT system execute software tests identify ICT system weaknesses implement ICT network diagnostic tools manage alarm system manage ICT legacy implication manage system testing perform ICT security testing solve ICT system problems use access control software	comply with legal regulations execute ICT audits manage IT security compliances migrate existing data provide ICT consulting advice

A summary of the essential and optional skills emerging from the selected ESCO profiles is provided in Table 15.

Table 15: Summary of the identified essential and optional skills.

Relevant essential skills	Relevant optional skills	Relevant essential and optional skills
administer ICT system	apply information security policies	address problems critically
analyse ICT system	comply with legal regulations	develop information security strategy
apply company policies	develop ICT test suite	ensure information privacy
apply ICT system usage policies	identify training needs	execute ICT audits

Relevant essential skills	Relevant optional skills	Relevant essential and optional skills
administer ICT system		execute software tests
conduct impact evaluation of ICT processes on business		identify ICT security risks
define security policies		identify legal requirements
educate on data confidentiality		implement ICT risk management
ensure adherence to organisational ICT standards		lead disaster recovery exercises
ensure compliance with legal requirements		manage changes in ICT system
establish an ICT security prevention plan		manage IT security compliances
identify ICT system weaknesses		migrate existing data
implement ICT network diagnostic tools		optimise choice of ICT solution
implement ICT recovery system		perform backups
maintain database security		perform ICT security testing
maintain ICT identity management		perform ICT troubleshooting
maintain plan for continuity of operations		provide ICT consulting advice
manage alarm system		
manage disaster recovery plans		
manage ICT legacy implication		
manage system security		
manage system testing		
perform risk analysis		
solve ICT system problems		
use access control software		

Annex C: Serious Games

Serious game development methodology

Drawing on past experience, serious game design methodologies have been proposed to effectively develop training for future ICT security experts.

In [GSV21] The methodology is organised in different points:

- Learning Objectives: the contents must be organised in areas, units and arguments. Guidelines provided help appropriate choices.
- Challenge design: the content must be based on the learning objectives previously selected. It is possible to design the challenges following a real attack life cycle (Initial compromise, Establishing Foothold, Privilege escalation, Internal Reconnaissance, Lateral Movement, Maintaining Presence, Completing the Mission). It is preferred to focus on the security problem instead of specific tools or programming languages. The game difficulty must progress rationally to avoid player frustration and time waste.
- Rules: clear definition of rules, specification of denied actions and possible countermeasures adopted.
- Hints: use of hints and help to avoid users frustration and blocking challenges. It is possible to use game mechanics to trigger hints (e.g. exploiting virtual coins)
- Game elements:
    - Narration: use the story as an accompaniment to the user during the game. It is possible to reflect the information known during an attack depending on the phase in which you are. It is suggested to use a brief story with a focus on important aspects to avoid boredom and distraction.
    - Injects, use notifications, messages, warnings to keep users' attention, time pressure and inform users about technical problems.
    - Player identity, create an identity for the player for example using an avatar, in which users can personalise themselves.
    - Rewards: recognise the user outcome with badges or points visible to other users.
- Technical Aspects: chose the technical aspect needed for the experience (for example virtual machine)
- Testing: test every aspect more than once before the official run.
- Data gathering and privacy: choose and implement elements to gather data needed to evaluate and control the project. However, it is important to keep into consideration the privacy issues and the GDPR policy. It is possible to use surveys pre and post-experience to collect feedback on the project.
- Evaluation: evaluating the project based on event logs, user perception and observation.

The development of a specific methodology to develop SSG is still an open research point, as is how to evaluate the breadth and depth of the knowledge transferred through such means. Presently SSG are gaining momentum, and now more data has to be gathered, adopting the available SSG in more educational context and training, and developing new ones tailored to specific contexts, to understand the usefulness of present games and how to improve them in the future ones.

Gamification and CTF

The vast majority of security violations are caused by human errors, due to very poor security awareness of normal users and by the increasing number of the social engineering components in the attack chain. So, increasing user's awareness and confidence regarding security issues is one of the most important components in the fight against cyberattacks and cybercrime.

As said, traditional security training programs mostly fail in raising skills and awareness, for several reasons, and to mitigate such issues the use of game elements in non-gaming contexts to increase motivation, involvement and stimulate a change of behaviour and habits (i.e. *gamification*) is a rich way under exploration. This technique has been applied in many different contexts from Education to Healthiness, and also in Cybersecurity.

One of the possible gamification approaches we focused on is the actual use of "games", in particular Serious Games. While another, briefly introduced to complete the panorama are Capture The Flag (CTF) competitions.

The capture the flag competitions are playful experiences, usually concentrated in one or a few days, to practise technical cybersecurity skills. Usually these are organised in teams competing or collaborating together, to find and/or defend the hidden flags using hacking techniques.

CTFs are targeted to players with a strong interest in the matter, otherwise, the game may result in a lot of frustration due to little progress in the game, because they require practical application of theoretical cybersecurity, often a non-trivial task. On the other hand, they allow a deep understanding of the mechanics of complex cybersecurity aspects (such as reverse engineering or encryption) and result in refined skills after a session.

Even if CTFs are suitable for many environments, the common application relates to computer security. CTFs can be organised internally but also by separate organisations, and participation may also be extended to external users or students.

To enrich and have a common base, preliminary training may be available before the competition. Typical goals are improved knowledge in network topology and network protocol, best-practice, communication protocols like IP, TCP, UDP, NAT, secure channel and standard techniques to achieve them (e.g. IPsec or TLS), software update, common attacks like DoS and MITM [AGA+17].

The most common CTFs types are:

- *Jeopardy*: usually online, to find the flag the players need to solve some challenges. More than one flag may be present in the game, and each flag gives to the team some points. At the end of the game, the team with the highest number of points wins. Usually, inside the team, cooperation is needed to divide the challenges and solve as many problems as possible in a limited time.
- *Attack/Defence*: each player/team has a virtual machine (VM). In this case, each team must defend its system (i.e. the VM) while attacking the others. The points are assigned on the base of the flag stolen in a limited time, and for a successful defence.
- *Boot2Root*: usually for individual users, the gamer has to exploit a vulnerability inside a virtual machine with the purpose to obtain root privileges.

Further, it is possible to mix them together with a high degree of flexibility.

Classical CTFs propose a multi-disciplinary mix of attracting aspects, i.e. game mechanics, physical interaction with tools and technology, competition between teams, socialisation and cooperation within the team, Furthermore, almost always the participation is voluntary, guaranteeing high levels of motivation.

CTFs are a successful method, so there exist platforms that use CTF schema to train their users (nowadays CTFs are often adopted to train future security experts). For example, ImmersiveLabs is a

platform used to empower organisations to increase, measure and demonstrate human capabilities on cybersecurity [IMM21]. It is continuously updated to provide fresh challenges for crisis simulations, it allows for Interaction, exploitation and incident simulation. Each simulation is set in different scenarios (e.g. a criminal organisation, a healthcare provider, an airport terminal). In this way, users approach different mindsets, and inside a scenario have to solve CTF-like tasks
To date, the main limit about topics covered by CTF is that usually, they are focused on the technical details leaving aside other important aspects in cybersecurity for example, organisational security and policy compliance. However, this is not an intrinsic limitation, so it is likely that future challenges will enrich the overall offer.

Examples of cybersecurity serious games

CRYPTOCLUB
https://www.cryptoclub.org/

On this site there are several sections containing very simple minigames to introduce players to the world of cryptography:

- Cypher tools: the practical operation of simple substitution encryption algorithms (including Caesar cypher and Vigènere cypher) is shown, both in the act of encrypting and in decrypting a message. There are also a couple of cracking tools based mostly on exploiting the frequency of letters in the English language to decrypt messages without the need for a key.
- Challenges: contains decryption challenges, provided frequently
- Games: find the downloadable game "VORTEX" whose first level is playable from the browser on the same page (Desert Oasis).
- Comics: contains a couple of comics dealing with the subject of cryptography.

In Vortex, there are three levels set in as many scenarios: *desert oasis, distant planet and abandoned mountain village*. The gameplay is based on a kind of treasure hunt in which you have to decode a message to reach the next one and get the final reward at the end of the level. The levels are respectively of easy, medium and hard difficulty, according to the algorithms required to solve the problems. There are no explicit systems for evaluating the player's learning, if not a simple score communicated at the end of the level. The game is aimed at young students. It is intended to be an educational tool to improve students' mathematical skills, showing them how simple mathematical operations are the basis of cryptography

CYBERCIEGE
https://nps.edu/web/c3o/downloads

It is a management game where the player must choose how to invest resources (game currency) to protect assets from cyber attacks implementing different countermeasures. The game proposes different levels addressing different cybersecurity topics. Initially, given the game complexity, appropriate actions are suggested by a tutorial. So, the player can familiarise themselves with the elements of the scenario. As the game progresses the levels become more complex introducing more in-depth concepts. A guide, always available on-demand, summarises and delves into the explanations provided by the tutorials.

The player is evaluated on the decisions made during the game, as these are saved in a log. The game is aimed to teach students the concepts of cybersecurity by letting them make decisions regarding the prevention and management of cyber threats in a business context.

A free copy (with limitations, such as not being able to save) is available here: https://nps.edu/web/c3o/downloads

BIGBRO
https://bitbucket.org/BlackDavid/securityseriousgame

It is a quiz game in which the player must correctly answer different types of questions:

- Multiple choice quiz with one or more selectable options
- Riddles where the purpose is to order a series of operations

The topics covered are general IT security concepts such as authentication, integrity, various cyber attacks, best known symmetric encryption algorithms, digital signatures.
The game itself is a tool for assessing the player's knowledge, as the answers given are recorded and displayed on a board in the form of statistics. Target Users are students who study the subject and who can, through quizzes, evaluate their knowledge.
The aim is to fix the theoretical concepts studied by the players. It has more of an educational purpose than an entertainment one.

CYBERCRAFT
https://github.com/luyangshang/CyberCraft

It is a turn-based strategy game that allows both the defender and attacker roles. The defender must protect his assets by investing his resources in various countermeasures, while the attacker must compromise the assets by bypassing or disabling the defences, deciding how to use his resources in the attack. The mechanics of cause and effect between attacks and countermeasures are clear and the game relies heavily on the entertainment offered by the challenge. It is possible to consult an in-game encyclopedia that lists the various attacks and defences in more detail.
The player performance is evaluated by a score based on the choices made by the player. Due to its structure, based more on playability than teaching, the game can attract a heterogeneous audience. The game goal is to introduce some cybersecurity concepts by emphasizing the attack-countermeasure relationship of the techniques described.

SIMSCADA
https://github.com/serranda/SecuritySeriousGame

It is a management/tycoon game, in which the player must manage the security of a company that works with SCADA systems. The player has to decide how to invest the funds at disposal, avoiding security breaches and keeping an active balance. During the game, the player reacts to unexpected attacks that hit the company. Thus, it learns how to prevent possible risks (even by following suggestions) before they can cause damage. The game provides an encyclopaedia in which some lessons are available on the topics covered. There are no in-depth technical aspects in the game mechanics, but rather the cause-effect-countermeasure relationships between security threats, attacks suffered and defence systems are

established. The choices and reaction times of the player are saved on the log (and some shown in the game). The log allows identifying signs of progress and topics to improve.
The game was mainly proposed to university students in computer science. The aim is to introduce the player to some security concepts in the context of SCADA systems

CENTIGRADE
https://cybersecurity.centigrade.de/

It is a game directly playable in a browser It consists of three minigames. The player is introduced to the game by a brief explanation of the mechanics and topics, plus some tips to prevent the threats faced in-game

- *Documents, please*: This is a timed game in which decisions must be made regarding the dissemination/destruction of documents. Based on the directives received and their content, these documents must be shared appropriately, also taking into account measures to strengthen the secrecy of documents (such as the use of encrypted emails). At the end of the level, the total score will be displayed, which depends on the number of documents examined and the accuracy of the decisions taken
- *Spam Defense*: the game consists of two parts, which deal with the topic of phishing from two different points of view. During the first part, the player has to play the role of an attacker who has to create phishing emails. To help the player, some information on the character of the victims is provided to apply some basic principles of social engineering. In the second part, the player has to catalogue some e-mails received. The player can choose whether it is a normal business email, if an email contains spam, or if the email is a phishing attempt. In the end, the overall score of the two parts is shown.
- *Hack the Planet*: in this minigame, the player impersonates a hacker. The goal is to find, through social media, personal information relating to an employee. The gameplay is simple: identify some keywords contained in the victim's posts and profiles by simply clicking on them. After this phase, the simulation of a brute-force attack is shown aiming to identify the passwords used by the victim, based on the information deduced from the social networks. The final score is then displayed, based on the number of information retrieved and the time to retrieve them.

At the end of each minigame, a score indicates the level of familiarity reached with the topic. The target audience is corporate employees with little cybersecurity knowledge, providing them basic information security training to company employees

DROPIT!
https://bitbucket.org/alexander_doni/dropit-a-personal-firewall-security-serious-game

It is a quiz game to which a platform-style has been applied. Before each level, the player is presented with the topics covered and is instructed on the possible threats that will arise. The player holds the role of newly hired IT security officer of the company. The environment in which it operates is a room in which there are six doors (three inbound and three outbound) and four mainframes, which represent the company's assets. The ports indicate the communication channels guarded by the firewall (role played by the player himself). The player will have to understand, by approaching the doors and evaluating the messages asking to enter and exit, what action to take to safeguard security without damaging the company's work (blocking or letting the messages pass). These messages are displayed within the game as individuals ask the player for permission to enter the mainframe room. If the player has allowed a

security threat to enter the room, it will approach one of the four mainframes and destroy it. If all mainframes are destroyed, game over occurs. Otherwise, once all the requests at the gates have been evaluated, the level will be completed and the end-of-level statistics will be shown. All the levels make up a short but appreciable story that unfolds until you reach one of the two possible endings.
The game has a data collection system, based on a database in which logs are collected with the choices made by the player and the scores achieved in the various levels. This allows you to evaluate the progress made at each level. The game is aimed at those who are already familiar information technology, and aims to to increase awareness of threats on the network. It is also aimed at those who do not give importance to computer security in personal devices. The goals are to raise awareness of the cyber security threats in everyday life and to introduce personal firewalls basics.

INSECTOR
https://github.com/davidpereza7/InSecTorv1

The game consists of multiple-choice quizzes with one or more correct answer options. The questions deal with basic attacks and related countermeasures to be adopted. The game itself is a tool for assessing the player's knowledge. It targets people, with little or no knowledge of cybersecurity, who need to learn basic knowledge to operate safely in the business environment. It has more of an educational purpose than an entertainment one.

GAME BASED SIMULATOR FOR TRAINING PROFESSIONAL IN CYBERSECURITY
http://gost.iitd.ac.in/serious_games/pages/ser.html

On this site, there are some browser minigames of various types concerning different aspects of IT security. The overall purpose is to provide basic knowledge on the main topics of cyber security, covering a large number of topics with a large number of games

Phishing: The game exposes players to phishing attacks to show them how they can protect their data from threats. The game is composed of only two very basic levels. The first shows an example of a malicious telephone call, aimed at acquiring the user's data. In the second, the player has to decide whether the emails that are displayed are "regular" emails or phishing attempts
Authentication: This game encourages users to avoid low-security passwords. The gameplay borrows the break-the-bricks style: the player must break all the bricks and collect or not the passwords that will fall later. The more complex a password is, the more points will be awarded, while if a password is too simple, points will be subtracted
Firewall: This game addresses some concepts regarding firewalls (using basic computer network concepts). Users are supported by tips and tutorials every time a new topic is introduced. The player has the objective of defending himself, through firewalls, from the attacks against him and at the same time must attack the adversarial network that is attacking him to end the attacks. The scenario presents a simulation of the functioning of computer networks, in which you can see the paths taken by the messages sent/received. The last level (without tutorial) introduces greater complexity because the requests that the player must satisfy lead to the creation of more rules applied to the various firewalls that must complete the task without damaging the previous functioning of the network
Blockchain: The purpose is to introduce how blockchains work.

Threat identification: This is to improve the ability of players to identify threats. In the first part of the game, phishing attempts via e-mail must be identified within a list of e-mails received, highlighting in detail the parts of the messages that seem suspicious. In the second part, the threat that is endangering the security of the company must be identified. In particular, the logs containing suspicious operations must be evaluated to reconstruct the attack preparation path that has been implemented, to prevent the actual attack from occurring
ARP spoofing: aims to show how the attack of the same name works. The active part of the game proposes a very short multiple-choice quiz regarding the operation and threats to the ARP protocol
There are also a group of simple games that have the same structure but deal with different vulnerabilities. The game is divided into two parts: the first is a multiple choice quiz in which questions relating to the topics covered by the game are formulated. The second part is a simulation in which the player must try to bring the attack to an end (not always very user-friendly, since no instructions are provided). Before addressing the two parts, it is possible to consult related documentation that details the topic at hand. Topics are: Components with known vulnerabilities, Cross-Site Scripting (XSS) Insufficient logging and monitoring, Sensitive data exposure.
Some other ones, along the same vein, are under development around the topics of malware incident forensics, cyber crisis management plan, password management, incident handling.

INTERLAND
https://beinternetawesome.withgoogle.com/it_it/interland

This game consists of a series of simple mini-games in different scenarios:

- *River of reality*: the goal is to learn to distinguish true from false. The minigame consists of crossing a river without falling into the water, by answering a multiple choice quiz.
- *Responsible upstream*: the goal is to learn how to use technology wisely. The minigame consists of sharing information with the right people, via a laser bouncing in a mirror system.
- *Treasure tower*: the goal is to learn how to keep personal information. The minigame consists in defending personal data from hackers who try to steal it, choosing the best passwords among those proposed.
- *Courteous reign*: the goal is to learn how to spread kindness online. The minigame consists of spreading positivity among users within a platform environment, avoiding and reporting individuals who have aggressive and negative attitudes.

After each minigame, there is a multiple-choice test that summarises the concepts addressed in the previous game. Each minigame provides a score. It targets children and teenagers (elementary and middle schools) to introduce a very young audience to the world of the web, focusing in particular on the dangers that moving online can entail and on the behaviours to be followed or avoided in the contexts of social networks or digital payments.

TARGETED ATTACKS
http://targetedattacks.trendmicro.com/

This game developed by Trendmicro is a visual novel consisting of short videos in which the actors participate, interspersed with sections where the player has to make a decision. This allows the game to be very immersive and realistic, and to have a good number of alternative scenarios. The player, who plays the CIO of the company, dictates the company's line of action, in particular concerning the area of IT security. Some limited funds are available to deal with the various problems encountered. The choices

made lead to a positive or negative ending, and then the player has the opportunity to retrace the choices, accompanied by a comment on their effectiveness and correctness. This game does not assess the player (apart from the auto-evaluation that a player may perform after the final comments). The main targets are potential buyers of TrendMicro services. The player is advertised about security issues and tools that can mitigate them, emphasizing the importance of managing corporate IT security with clarity and competence.

DATA CENTER ATTACK

https://resources.trendmicro.com/datacenter-attack.html

Another game from TrendMicro with similar gameplay. In this case, the player is the CISO of a hospital, thus having to make choices to manage the safety of the structure.

CYBERSECURITY LAB

https://www.pbs.org/wgbh/nova/labs//lab/cyber/research

The player must manage the growth of a new social network and consequently defend himself from a series of increasingly sophisticated attacks against his start-up. The gameplay is made up of minigames that deal with different themes:

- *Programming*: the player must program the movements of a robot to solve a maze, placing some blocks of pseudo-code in the right order.
- *Passwords*: these are a series of duels with a hacker. The player must adopt passwords that are complex enough to not be discovered by the opponent. At the same time, the password created by the opponent must be guessed, based on the clues provided.
- *Social engineering*: pairs of emails or internet pages are presented, one of which is reliable while the other is a phishing attempt. The player must identify the differences between the two and decide which one they consider the phishing attempt to be.
- *Network attacks*: the player must defend the start-up from attacks, investing what he has earned in previous mini-games in purchasing adequate defences.

A report at the end (if the user is registered) indicates how much has been completed. There are also some video quizzes (https://www.pbs.org/wgbh/nova/labs/lab/cyber/1/1/) to check how well the topics have been understood. It targets middle and high school students to teach how to defend their personal information in the digital world, detect phishing attempts, learn programming basics and defend against cyber attacks.

DATA-DRIVEN SECURITY GAME

https://github.com/dagerikhl/ddsg

It is a “defend the tower” type game in which the player has to defend 3 entry points from enemy attacks: *client*, *network* and *server*. The player must deploy the appropriate defence to neutralise specific attacks. In the gameplay, specific turrets (defences) can hit only specific enemies (cyber-attacks). At the end of the game, questionnaires were submitted to users to evaluate the effectiveness of the title. The audience are IT students who have received basic notions on computer security or who are interested in the subject, and this game may provide introductory knowledge about cyber attacks and how to avoid/mitigate them.

NETSIM
https://netsim.erinn.io/

It is a computer network simulator, in which it is possible to send and receive packets within the fictitious network. The levels are structured incrementally and show (after introduction) possible attacks that can be perpetrated on the network. At the beginning of each level, some indications are provided to successfully complete the level. There is no player rating of any kind. The main targets are young students with no particular knowledge in computer science aiming to transmit basic hacking principles and stimulate interests in computer security.

PERMISSION IMPOSSIBLE
https://groups.inf.ed.ac.uk/tulips/projects/1617/PermissionImpossible/

A simple game divided into a set of levels. The player builds the input and output rules of a firewall. The bricks must be dragged in a row to form the rules. Finally, questionnaires were submitted to users to evaluate the effectiveness of the title. The targets are young students, possibly already interested in cybersecurity, to teach the basics of how a firewall works.

THE WEAKEST LINK
https://www.isdecisions.com/user-security-awareness-game/

The protagonist is a new employee and has to answer a multiple-choice question every working day for a month. Each answer is communicated whether the selected one is correct or not, with a brief explanation of its implications. In the end, the level of safety achieved based on the decisions taken is indicated. The game is made by the company IsDecisions, which deals with computer security in the context of user access and authorization. The purpose of the game is to show to potential buyers (but can potentially raise security awareness in anyone) how the employee choices may affect the security of an organisation (particularly in the area in which the game developer operates).

Annex D: Impact and integration of research and innovation

This appendix provides a detailed mapping of the knowledge areas identified in the CyberSec4Europe Knowledge Framework to the various tasks analysed in WP3 and WP5. These work packages are in charge of the research and innovation initiatives of CyberSec4Europe, which have both short- and long-term impact into the education curricula and training of cybersecurity personnel. This annex describes in detail how the demonstrators and research initiatives studied in WP3 and WP5 relate to different educational areas, following the classification of the CyberSec4Europe framework [D6.2]. For a high level overview of which tasks involve which knowledge area, we refer to tables 9 and 10 in Section 3.2 for WP3 tasks and WP5 tasks, respectively.

This appendix is organised by knowledge area. For each task involved in that knowledge area, the specific relevance is discussed in a short paragraph.

Data Security

T3.2 – Research and Integration on Cybersecurity Enablers and underlying Technologies
This task discusses techniques and tools for enhancing confidentiality, integrity, availability of data stored in public systems (e.g. Argus). Approaches for data privacy, privacy-aware aggregation, data anonymization (DANS), privacy-preserving for genomic data (PP4Genomic) Authorization management, and GDPR-by-design(GENERAL_D).

T3.3 – SDL: Software Development Lifecycle
This task discusses tool-supported approaches for credential hardening (HONEYGEN, MODSSL-HMAC), privacy analysis in workflows and dataflows (PLEAK), verification of confidentiality and privacy in protocols (PVS), and enforcement of privacy policies, and verified access control (SYSVER,VEREFOO) as reported in [D3.9] and [D3.15].

T3.4 – Security Intelligence
This task discusses teaching data protection and anonymization techniques to store and share sensitive cyber threat intelligence information in a privacy-preserving manner, as implemented in TATIS ([D3.3] and [D3.14]).

T3.9 – Continuous Scouting
TEEs & software protections can be used to increase data privacy during the computations [D3.10].

T5.1 – Open Banking
The OBSIDIAN fighting fraud demonstrator goes to great pains to protect potentially fraudulent IBANs through pseudonymisation techniques (hash plus encryption) both at rest and on every occasion an OBSIDIAN participant chooses to transmit the data across the network [D5.2, D5.5].

T5.2 – Supply Chain
The supply chain security demonstrator illustrates how data can be stored securely in a distributed architecture. Both use cases of the demonstrator apply blockchain technology and demonstrate how information can be securely exchanged as well as stored and managed in a distributed ledger. Furthermore, immutability of data and non-repudiation of actions are key properties that are presented [D5.2, D5.5].

T5.3 – Privacy-preserving Identity Management
By actively contributing to data minimization, this demonstrator increases the security of personal data as unnecessary sharing of data is avoided. Furthermore, high data quality is ensured by giving formal end-to-end authenticity guarantees [D5.2, D5.5].

T5.6 – Medical Data Exchange
Through the use of anonymization tools and cryptographic techniques such as Functional encryption, data is protected at any moment during the data exchange process [D5.2, D5.5].

Software Security

T3.3 – SDL: Software Development Lifecycle
This task discusses tool-supported proactive approaches to secure lifecycle development [D3.9, D3.15], including security requirements and design patterns (SEMCO), threat modelling (CORAS, BOWTIE-PLUS, RISQFLAN), formal verification of security policies (VEREFOO, SYSVER, PVS), security & privacy analysis (HERMES, VTPIN, PLEAK), and software hardening (MODSSL-HMAC and HONEYGEN, SEMCO).

T3.6 – Usable Security (Human-centred Cybersecurity)
In this task, it is proposed to teach effective measures to improve the usability of security and privacy technologies and what security and privacy technologies have (and have not) gained user adoption [D3.5, D3.7].

T3.8 – Conformity, Validation and Certification
Software certification can be used as part of the development process to ensure security properties [D3.8, D3.22].

Component Security

T3.3 – Conformity, Validation and Certification
This task discusses vulnerability analysis techniques with tools like HERMES and VTPIN.

T3.8 – Conformity, Validation and Certification
Components can be certified separately, the testing and management process can be supported with the framework and certification assistant tool proposed in [D3.8] and [D3.22].

T5.4 – Conformity, Validation and Certification
The incident reporting platform for the financial sector demonstrator has been designed in a modular way, around the open-source tools TheHive and Cortex, so that it can be easily extended or adapted in the future. In particular, in the same way that WP3 assets have been integrated as Cortex analyzers and specific functionalities of the platform provided as Cortex responders, other security assets or analyzers could be integrated in the platform. Connection of these tools with MISP also provides additional features for threat intelligence data sharing. See also [D5.2, D5.5].

T5.4 – Conformity, Validation and Certification
The maritime transport security demonstrator involves the development of various security services ranging from threat modelling and risk assessment, hardware security, secure communications and maritime PKI services. Each security service is implemented as a different security module. The integration among the security modules enhances the security services in several ways: risk assessment services are enhanced with the application of security hardening mitigation controls, while the secure maritime communications are enhanced by the use of the maritime PKI services. See also [D5.2, D5.5].

T5.4 – Conformity, Validation and Certification
As the anonymisation and encrypted tools are provided as a service the web access is secured through HTTPS by configuring TLS/SSL. Additionally, the support of CORS mechanisms is implemented for interaction between the browser and the server. The modular design of these components allows for access control mechanisms such as IP filtering, giving access only to those registered users. From a maintenance perspective, the components are updated with the latest versions of the libraries from third parties, and updating libraries when secure vulnerabilities are detected is supported. See also [D5.2, D5.5].

Connection Security

T3.2 – Research and Integration on Cybersecurity Enablers and underlying Technologies
This task discusses approaches to strengthen security, scalability, consensus, trust and privacy in

blockchain platforms, privacy-preserving solutions for distributed computations on potentially sensitive data, and confidential analysis of data from multiple parties (Sharemind).

T3.3 - Conformity, Validation and Certification
This task discusses approaches for modelling and verifying secure communication protocols with automated tools like the protocol verification suite PVS [D3.9, D3.15].

T3.5 - Adaptive Security
This task discusses teaching novel techniques to adaptively configure network security policies depending on changing network vulnerabilities, introduced for example by a changing network topology. Such techniques can be exemplified using the adaptive risk assessment asset (SYSVER) developed in [D3.21].

T5.1 - Open Banking
The OBSIDIAN network relies on a central OBSIDIAN server to route communications about potential fraudulent IBANs between participating financial institutions. This central server only stores logistical transaction data but no actual banking data. It is also responsible for ensuring that none of the participants know with whom they are communicating or have been communicated by. See also [D5.2, D5.5].

T5.2 - Supply Chain
The demonstrator illustrates how a decentral, distributed architecture (without the need for a trusted third party) can be set up and secure connections between infrastructures of cooperating organisations can be set up. Among others, aspects like secure communication, identity/credential management are addressed. See also [D5.2, D5.5].

System Security

T3.1 – Common Framework Design
This task proposes a definition of collection of assets covering the different components of a cybersecurity system [D3.1, D3.12].

T3.2 – Research and Integration on Cybersecurity Enablers and underlying Technologies
This task discusses tools for elastic deployment of TEE-based applications in the cloud (ReplicaTEE) that protect privacy, as well as backdoor-resistant TEEs.

T3.3 – SDL: Software Development Lifecycle
This task discusses approaches for guaranteeing correct and efficient implementations of network security policies as supported by tools like VEREFOO and SYSVER [D3.9, D3.15].

T3.5 – Adaptive Security
This task discusses teaching novel methods to elicit and prioritise emerging security threats using a behavioural model of a system (e.g., a data flow diagram). These methods can be illustrated based on the situation-driven adaptive risk and security enforcement assets (SPARTA, MITIGATE, DynSMAUGconcepts) developed in [D3.21].

T3.7 – Regulatory Sources for Citizen-friendly Goals
This task discusses eIDAS interoperability and cross-border compliance issues [D3.18], and analyses identification and authentication methods used in the implementation of eIDAS nodes (Authentication methods and Identity).

Human Security

T3.2 – Research and Integration on Cybersecurity Enablers and underlying Technologies
Relevant discussions in this task include the following: approaches and tools for privacy-preserving (minimal disclosure and unlinkability) authentication (presentation of attributes) (assets such as pp-

IDM and Issuer-Hiding Anonymous Credentials), passwordless authentication and device-centric authentication solutions, privacy-friendly identity management in the Cloud, Interoperability and cross-border eIDAS compliance, and Guidelines for the General Data Protection Regulation (GDPR).

T3.5 – Adaptive Security
This task discusses teaching novel approaches to engineer adaptive authentication systems that can adapt depending on changing contextual factors and varying priorities of relevant and potentially conflicting requirements, such as security, usability and performance. These approaches can be illustrated using the adaptive authentication assets developed in [D3.21].

T3.6 – Usable Security (Human-centred Cybersecurity)
This task proposes new tools and concepts for improving usability for privacy preservation, authentication, risk assessment, and more [D3.16].

T3.7 – Regulatory Sources for Citizen-friendly Goals
GDPR Guidelines and DPIA Template [D3.6] are ultimately tools to reduce user burden and decisions, provide secure defaults, reduce unintentional errors, and make threats along with risks contextual and concrete when ensuring GDPR compliance and performing a DPIA (Usable Security and Privacy => Design guidance and implications).

T3.9 – Continuous Scouting
This task discusses new AI-based social engineering attacks [D3.10].

T3.10 – Impact on Society
Cybersecurity awareness is directly connected to protecting the human factor in cyberspace.

T5.1 – Open Banking
According to French and other Member States' laws, the identity of everyone, including fraudsters, falls under the remit of GDPR. In particular, in France an IBAN is considered to be a potential PII and consequently OBSIDIAN ensures that the actual IBAN itself is not revealed (i.e., decipherable) by any of the OBSIDIAN participating financial institutions to any of the others. In addition, although the rules differ across Member States, banking secrecy, the banking community's equivalent of a Hippocratic oath not to reveal confidential account information, is enshrined in law. See also [D5.2, D5.5].

T5.3 – Privacy Preserving Identity Management
The privacy-preserving identity management demonstrator is developing and advancing cryptographic mechanisms that put users back into control over their personal data, but letting them, on a fine granular level, decide which information they want to share and which information to keep confidential, without negatively impacting the authenticity of the revealed information. Furthermore, different actions of the same user remain unlinkable, thereby reducing the risk of user profiling. The specific use case focuses on data minimization during job application processes, but the technology can easily be used also in other contexts. See also [D5.2, D5.5].

T5.6 – Medical Data Exchange
This pilot shows how to protect sensitive health data during the data exchange process, by using privacy-preserving techniques such as anonymisation or cryptographic techniques. Additionally, strong authentication mechanisms (eIDAS, eID) are integrated for data access control and facilitating cross-border interoperability. See also [D5.2, D5.5].

T5.7 – Smart Cities
The smart cities demonstrator cases have been focused on setup and put in operation a user centric infrastructure to support sensors and other urban data platforms and infrastructure for identity and personal data exchange and their reuse in public services, in compliance with GDPR. See also [D5.2, D5.5].

Organisational Security

T3.1 – Common Framework Design
This task includes a framework definition to define the properties and requirements of security and privacy of cybersecurity systems [D3.1].

T3.3 – SDL: Software Development Lifecycle
In this task, threat modelling and assessment tools like CORAS, BOWTIE-PLUS and RISQFLAN [D3.9, D3.15] are discussed.

T3.4 – Security Intelligence
This task discusses teaching analytical tools for monitoring security can benefit from the concepts and implementation of intrusion detection components that use packet-level properties of network traffic (from cloud to edge nodes) and AI technologies such as ENIDS [D3.3, D3.12]

T3.10 – Impact on Society
The provided conceptual framework for cybersecurity awareness has considered the organisation's needs and expectations from their awareness initiatives and has also answered how they can be achieved optimally.

T5.4 – Incident Reporting
The Incident Reporting Platform demonstrator (focused on the financial sector) is also connected to threat intelligence platform (MISP) to provide the possibility to share information about cyber incidents in a privacy-preserving manner inside the own organisation or with others, and score incoming indicators of compromise to evaluate their reliability and actionability. See also [D5.2, D5.5].

T5.5 – Maritime Transport
The MITIGATE risk assessment tool, which is integrated and extended in the maritime transport demonstrator, can be used to assist organisations in the maritime sector to identify and assess their cybersecurity threats and risks. See also [D5.2, D5.5].

T5.7 – Smart Cities
The smart cities demonstrator cases have been focused on the setup of an Open Innovation cycle that will drive city stakeholders from cyber security risks and needs assessment to the identification of cyber posture to prevent cybersecurity attacks. See also [D5.2, D5.5].

Societal Security

T3.2 – Research and Integration on Cybersecurity Enablers and underlying Technologies
By researching and developing privacy-enhancing technologies, this task contributes to the central right of privacy in an online world.

T3.7 – Regulatory Sources for Citizen-friendly Goals
GDPR heterogeneity (D3.18) looks at GDPR-related legislation in the EU Member States and analyses their differences (Cyber Law => Cross-border privacy and data security laws).

T3.10 – Regulatory Sources for Citizen-friendly Goals
The provided conceptual framework and guidelines for cybersecurity awareness could guide in designing effective awareness campaigns for the general public.

T5.3 – Privacy Preserving Identity Management
The demonstrated technology directly contributes to increased privacy in an online world. The specific use case also helps to reduce discrimination (e.g., age, nationality, gender). See also [D5.2, D5.5].

T5.5 – Maritime Transport
As transportation is a recognised critical sector for the EU, the security services developed in this task

will directly contribute in better understanding and assessing security risks in the critical sector of maritime transport. See also [D5.2, D5.5].

Operate and Maintain

T3.5 - Adaptive Security
This task discusses teaching adaptive approaches to adjust incident reporting procedures and methods depending on the applicable regulatory bodies. These approaches can be illustrated using the AIRE asset developed in [D3.21], which can adaptively change the incident reporting workflow and template depending on the jurisdiction of the organisation reporting a security incident.

T3.8 – Conformity, Validation and Certification
The testing, management and certification process of software and its components can be supported with the framework and certification assistant tool in [D3.8, D3.22].

T5.4 – Security Intelligence
The Incident Reporting Platform demonstrator (focused on the financial sector) helps the organisations in the mandatory incident reporting process that need to follow to report cybersecurity incidents to the relevant authorities to be compliant with different regulations. See also [D5.2, D5.5].